E1 Unico Corporation

Access Controls 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 enforces a comprehensive, layered access control framework across all production systems, cloud infrastructure, and sensitive data. Access to production assets — physical or virtual — is restricted by design through documented policies, role-based enforcement, zero trust architecture, and centralized identity management. All controls are continuously reviewed, audited, and updated to reflect the current threat landscape.

✓ DOCUMENTED POLICY

A formally defined Access Controls Policy governs all access to production assets and sensitive data across the organization.

✓ ROLE-BASED ACCESS CONTROL

RBAC is enforced across all platforms. Users receive the minimum permissions required for their role — nothing more.

✓ PERIODIC ACCESS REVIEWS

Access rights are reviewed quarterly. Stale, excess, or inappropriate access is revoked promptly following each review cycle.

✓ AUTOMATED DE-PROVISIONING

All access credentials are revoked automatically within 24 hours of employee termination or role transfer — no manual steps required.

✓ ZERO TRUST ARCHITECTURE

No implicit trust is granted based on network location. Every request is authenticated and authorized independently, regardless of source.

✓ CENTRALIZED IAM

All identity and access management is centralized through Vercel, GitHub, and NextAuth.js — providing a single control plane for all access.

✓ OAUTH TOKENS & TLS CERTIFICATES FOR NON-HUMAN AUTHENTICATION

All service-to-service authentication (Plaid, Stripe, Twilio, internal APIs) uses OAuth 2.0 tokens or TLS mutual authentication — never static passwords or shared credentials.

1. Scope

This policy applies to all access to:

- UnicoOS production application (os.e1unico.com) and all associated APIs
- Cloud infrastructure: Vercel (hosting), Neon (PostgreSQL database), GitHub (source code)
- Third-party integrations: Plaid, Stripe, Twilio, and all connected services
- All customer financial data, PII, and confidential business records
- All employees, contractors, administrators, and automated systems

2. Defined & Documented Access Control Policy

E1 Unico Corporation maintains a formally documented access control policy that is:

- Reviewed and approved by the CEO annually or after any significant security event
- Communicated to all team members and contractors upon onboarding
- Available to auditors and regulatory reviewers upon request
- Versioned and maintained in the company's secure document repository

3. Role-Based Access Control (RBAC)

3.1 Principle of Least Privilege

All access rights are granted based on the principle of least privilege. Users, services, and automated systems receive only the permissions required for their specific function — and no more. Broad or administrative access requires explicit approval from the CEO.

3.2 Access Tiers

Role	Access Level	Scope
Super Admin (CEO)	Full	All systems, all data, all configurations
Platform Admin	High	Application configuration, user management
Staff / Operator	Standard	Assigned modules only — no system config access
Client / End User	Restricted	Own account data only — fully isolated per tenant
Automated Services	Scoped	API-specific OAuth scopes — no broad access

3.3 Multi-Tenant Isolation

UnicoOS enforces strict multi-tenant database partitioning. Each client account's data is logically isolated by `subAccountId` at every database query level. No cross-account data access is architecturally possible without explicit authorization.

4. Periodic Access Reviews & Audits

- **Quarterly:** Full review of all user accounts, roles, and permissions across Vercel, GitHub, Neon, and

integrated services

- **Annually:** Comprehensive access audit including third-party integrations and API key rotation review
- **On-demand:** Immediate access review triggered by any security incident, personnel change, or role modification
- Audit logs are retained for a minimum of 12 months and are available for regulatory review
- Any access that cannot be justified by current role requirements is revoked during each review cycle

5. Automated De-Provisioning

E1 Unico Corporation enforces automated access revocation to eliminate the risk of orphaned credentials:

- All platform accounts (Vercel, GitHub, Neon, third-party services) are de-provisioned within **24 hours** of employee termination or role transfer
- API keys and OAuth tokens issued to departing team members are rotated immediately upon separation
- De-provisioning is tracked via a documented offboarding checklist completed by the CEO
- Session tokens are invalidated server-side — users cannot maintain access after revocation

6. Zero Trust Access Architecture

UnicoOS operates on a Zero Trust model — no user, system, or network location is implicitly trusted:

- **Verify explicitly:** Every API request is authenticated via session token or OAuth credential before any data is returned
- **Least privilege access:** Authorization checks are enforced at the API layer on every request — not assumed from login state
- **Assume breach:** All systems log access events as if compromise is possible — anomalous patterns trigger alerts
- Internal services authenticate to each other via scoped OAuth tokens — no internal network is treated as trusted
- All database access requires a valid authenticated session with a verified `subAccountId` — no raw database exposure

7. Centralized Identity & Access Management

All identity and access management for UnicoOS is centralized through a unified control plane:

- **NextAuth.js:** Centralized authentication for all user sessions — handles login, session management, and token lifecycle
- **Vercel Dashboard:** Single point of control for all deployment access, environment secrets, and team permissions
- **GitHub:** Repository access managed with branch protection, required reviews, and team-scoped permissions
- **Neon:** Database credentials managed centrally — connection strings stored as encrypted environment variables only
- All service credentials are stored in Vercel's encrypted environment variable vault — never hardcoded or committed to source control

8. OAuth Tokens & TLS Certificates for Non-Human Authentication

8.1 Service-to-Service Authentication

All automated and non-human system authentication uses industry-standard token-based methods:

Integration	Authentication Method	Scope
Plaid API	OAuth 2.0 — Client ID + Secret + User-scoped Access Token	Per-user, per-institution — minimum required scope
Stripe API	Bearer token (Restricted API Key)	Payment processing only — no customer data read
Twilio API	Account SID + Auth Token over HTTPS	SMS/Voice only
GitHub Actions	Short-lived OIDC tokens	Deploy pipeline only
Neon Database	TLS-encrypted connection string	Application service role only
Vercel API	Scoped deployment tokens	Deployment and env var management only

8.2 Token Management

- All API tokens and secrets are rotated at minimum annually or immediately upon any suspected compromise
- Plaid access tokens (user bank connections) are stored encrypted at rest and never logged
- No static passwords are used for service-to-service communication
- All external API calls are made exclusively over TLS 1.3

9. Physical Access Controls

UnicoOS is a cloud-native platform with no on-premises servers. Physical security is delegated to SOC 2 Type II certified infrastructure providers:

- **Vercel** — SOC 2 Type II certified data centers with physical access controls, surveillance, and biometric entry
- **Neon** — SOC 2 Type II certified, hosted on AWS infrastructure with enterprise-grade physical security
- No E1 Unico personnel have physical access to production server hardware — access is exclusively virtual and authenticated

10. Authentication Standards

- All administrative accounts require **Multi-Factor Authentication (MFA)** — no exceptions
- Minimum password length: 16 characters with complexity requirements
- Password reuse prohibited — unique credentials required per service
- Session tokens expire after inactivity — users must re-authenticate
- Failed login attempts are rate-limited and logged

Policy Approval

This Access Controls Policy has been reviewed, approved, and is actively enforced across all E1 Unico Corporation platforms as of the effective date below.

Authorized Signatory | Date | Next Review Date

Manuel Montemayor Jr., Founder & CEO
E1 Unico Corporation

Annual review — June 2027