E1 Unico Corporation

Information Security 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

EXECUTIVE POLICY STATEMENT

UnicoOS maintains a comprehensive, documented Information Security Policy (ISP) framework that has been fully operationalized across our multi-tenant SaaS architecture. This policy outlines the systemic administrative, technical, and physical safeguards implemented to protect client-permissioned financial data and system infrastructure from unauthorized access, disruption, or exposure.

Our operationalized procedures are structured around three core pillars to manage risk continuously:

IDENTIFICATION

Automated vulnerability scanning, code dependency checks, and continuous asset profiling within our unified cloud environment to detect potential security weaknesses or misconfigurations before they can be exploited.

MITIGATION

Strict enforcement of Least Privilege access controls, end-to-end data encryption (AES-256 at rest and TLS 1.3 in transit), automated IP throttling, and isolated multi-tenant database partitioning to contain risks natively.

MONITORING

Real-time event logging and centralized log auditing for all data access requests, integrated with automated alert workflows that instantly flag anomalous network activity or unverified cross-account traffic to platform administrators.

1. Scope & Applicability

This policy applies to:

- All employees, contractors, and authorized users of E1 Unico Corporation systems
- All digital platforms operated by E1 Unico Corporation, including UnicoOS (os.e1unico.com)
- All third-party integrations and data processors (Plaid, Stripe, Twilio, Vercel, Neon, etc.)
- All customer data, financial data, and personally identifiable information (PII)

- Subsidiaries: Industrial Drip LLC, Ultra Plant Services, Feast and Fun LLC

2. Data Classification

Classification	Description	Examples
Confidential	Highly sensitive — restricted access only	Bank tokens, API secrets, user credentials, PII
Internal	Business use only	Customer records, invoices, financial data
Public	Safe for public disclosure	Marketing materials, public website content

3. Access Control

- All systems enforce role-based access control (RBAC) with the principle of least privilege
- Administrative accounts require strong, unique passwords (minimum 16 characters)
- Multi-factor authentication (MFA) is mandatory for all cloud service logins (Vercel, Neon, Plaid, Stripe, GitHub)
- Multi-tenant database partitioning ensures no cross-account data exposure
- Access credentials are revoked immediately upon employee or contractor separation
- Automated IP throttling and rate-limiting is applied to all API endpoints

4. Financial Data & Plaid Integration Security

4.1 Plaid Bank Account Linking

- OAuth-based linking — E1 Unico Corporation never stores or transmits bank login credentials
- Plaid access tokens encrypted at rest using AES-256 in our isolated database
- All token exchange operations are performed server-side exclusively — never client-exposed
- All Plaid API calls are made exclusively over TLS 1.3 encrypted connections
- Client-permissioned data is scoped to the minimum required for the stated use case

4.2 Stripe Payment Processing

- Payment card data is never stored, processed, or transmitted through E1 Unico servers
- All payment operations are delegated to Stripe's PCI-DSS Level 1 infrastructure
- Webhook authenticity is verified via Stripe signature validation on every inbound event

5. Technical Security Controls

5.1 Encryption Standards

- **At rest:** AES-256 encryption at the database layer (Neon PostgreSQL)
- **In transit:** TLS 1.3 enforced on all production connections
- **Secrets management:** All API keys and credentials stored as encrypted environment variables — never in source code or version control

5.2 Application Security

- Authentication via NextAuth.js with secure, short-lived session tokens
- All user input validated and sanitized server-side before processing
- SQL injection prevented via Prisma ORM parameterized queries

- Passwords hashed using bcrypt with a minimum of 12 salt rounds
- HTTPS enforced on all production URLs with HSTS headers
- CSP (Content Security Policy) headers applied to all responses

5.3 Infrastructure Security

- Application hosted on Vercel (SOC 2 Type II certified, global edge network)
- Database hosted on Neon (SOC 2 certified, encrypted at rest and in transit)
- Source code in private GitHub repository with branch protection and required reviews
- Automated dependency vulnerability scanning via GitHub Dependabot

6. Monitoring & Incident Response

6.1 Continuous Monitoring

- Real-time event logging and centralized log auditing for all data access requests
- Automated alert workflows for anomalous network activity or unverified cross-account traffic
- Application error monitoring and performance tracking via Vercel Analytics
- Database query auditing for unauthorized access patterns

6.2 Incident Response Procedure

1. **Detect & Contain** — Identify the incident and isolate affected systems within 1 hour
2. **Assess** — Determine scope, affected data, and potential impact
3. **Notify** — Inform affected customers within 72 hours per applicable law and Plaid policy
4. **Remediate** — Patch vulnerabilities, rotate credentials, restore services
5. **Review** — Conduct post-incident review and update policy within 30 days

Security incidents: **Unico@E1Unico.com** | Response SLA: Critical issues within 24 hours

7. Authorized Subprocessors

Vendor	Purpose	Certification
Vercel	Application hosting & edge network	SOC 2 Type II **Certified**
Neon	PostgreSQL database	SOC 2 Type II **Certified**
Plaid	Bank account linking	PCI DSS, SOC 2 **Certified**
Stripe	Payment processing	PCI DSS Level 1 **Certified**
Twilio	SMS / Voice communications	SOC 2 Type II **Certified**
GitHub	Source code & version control	SOC 2 Type II **Certified**

8. Compliance Framework

- **Gramm-Leach-Bliley Act (GLBA)** — Safeguarding customer financial information
- **Texas Business & Commerce Code §521** — State data breach notification requirements
- **Plaid Developer Policy** — Terms governing use of Plaid APIs and customer financial data
- **Stripe Services Agreement** — Terms governing payment processing and data handling

- **OWASP Top 10** — Web application security best practices applied in development

Policy Approval

This Information Security 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