🛡

E1 Unico Corporation

Vulnerability Management 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 operates a continuous vulnerability management program across all production assets, cloud infrastructure, source code dependencies, and end-user systems. This program actively identifies, prioritizes, and remediates security vulnerabilities before they can be exploited — with defined SLAs for every severity level. All end-of-life software is tracked and replaced proactively.

🔍 SCAN

Automated continuous scanning of all production assets, source code dependencies, and infrastructure for known vulnerabilities and misconfigurations.

⚡ PATCH

All identified vulnerabilities are triaged by severity and remediated within defined SLA windows — Critical within 24 hours, no exceptions.

♻ MONITOR EOL

All runtime environments, libraries, and dependencies are tracked for end-of-life status. EOL software is replaced before support expires.

1. Scope

This policy applies to all systems that store, process, or transmit consumer financial data or support UnicoOS operations:

- Production application infrastructure (Vercel edge network)
- Production database (Neon PostgreSQL)
- Application source code and all third-party dependencies (npm packages)
- CI/CD pipeline (GitHub Actions)
- All developer and contractor machines used for production work
- All third-party integrations (Plaid, Stripe, Twilio)

2. Vulnerability Scanning

2.1 Automated Dependency Scanning

- **GitHub Dependabot** — Continuously scans all npm dependencies in the UnicoOS repository against the National Vulnerability Database (NVD) and GitHub Advisory Database
- Dependabot automatically creates pull requests to update vulnerable dependencies — reviewed and merged within the applicable SLA
- All Dependabot alerts are triaged by the CEO within 24 hours of notification

2.2 Code Security Scanning

- **GitHub CodeQL** — Static application security testing (SAST) runs on every pull request and commit to the main branch
- Scans detect common vulnerabilities including SQL injection, XSS, insecure deserialization, and hardcoded secrets
- No code with unresolved Critical or High findings is merged to production

2.3 Secret Scanning

- GitHub secret scanning is enabled on the repository — automatically detects accidentally committed API keys, tokens, and credentials
- Any detected secret is immediately rotated and invalidated — regardless of whether it was ever exposed

2.4 Infrastructure Scanning

- Vercel's built-in security monitoring continuously audits the production deployment environment
- npm audit runs automatically on every deployment build — deployment fails if Critical vulnerabilities are unresolved

3. Patching SLA — Defined Remediation Timeframes

Severity	CVSS Score	Description	Remediation SLA
Critical	9.0 – 10.0	Remote code execution, authentication bypass, data exposure risk	**Within 24 hours**
High	7.0 – 8.9	Significant risk — privilege escalation, data integrity issues	**Within 7 days**
Medium	4.0 – 6.9	Limited exploitability, requires specific conditions	**Within 30 days**
Low	0.1 – 3.9	Minimal risk — informational or theoretical exposure	**Within 90 days**

If a patch is not yet available for a Critical or High vulnerability, a compensating control (network isolation, feature disable, WAF rule) is applied within the same SLA window while awaiting vendor remediation.

4. End-of-Life (EOL) Software Management

4.1 Runtime Environments

Component	Current Version	EOL Tracking	Status
Node.js	v22 LTS	nodejs.org/en/about/releases	✓ Active LTS

Next.js	15.x	GitHub release schedule	✓ Current
React	19.x	react.dev changelog	✓ Current
PostgreSQL (Neon)	Managed — auto-updated	Neon-managed	✓ Managed

4.2 EOL Policy

- All runtime environments must be on a supported LTS release — EOL versions are upgraded within 30 days of end-of-support announcement
- Third-party npm dependencies are reviewed monthly for deprecation and EOL status
- Dependabot version update PRs are reviewed and merged within 14 days for non-security updates
- Any dependency that has been abandoned (no updates in 2+ years, known vulnerabilities unpatched) is replaced with an actively maintained alternative

5. Vulnerability Tracking & Reporting

- All identified vulnerabilities are logged in the GitHub Security tab with severity, status, and assigned remediation date
- Vulnerability status is reviewed weekly by the CEO as part of routine security operations
- Unresolved vulnerabilities past their SLA window are escalated immediately and treated as security incidents
- Quarterly vulnerability summary reports are maintained for audit purposes

6. Developer Security Practices

- All code changes require pull request review before merging to the main branch
- Branch protection rules prevent direct commits to main — all changes go through CI/CD with security checks
- OWASP Top 10 guidelines are followed in all application development
- Secrets are never committed to source control — enforced by pre-commit hooks and GitHub secret scanning
- All developer machines run current, supported operating systems with automatic security updates enabled

Policy Approval

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

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