SECURITY POSTURE

Architecture, controls, sub-processors

NOCTARA, INC. . PUPUL, INC. . MARIETTA, OHIO

EFFECTIVE 2026-05-16

For procurement, InfoSec, and legal review. Updated 2026-05-09. *DRAFT.*

WHAT WE ARE

Noctara, Inc. is a Delaware C-Corp operating subsidiary of Pupul, Inc. We build behavioral identity infrastructure: an instrument that reads how people type to produce one diagnostic word about who they are. Customers buy our product LUX (consumer) and VEX (team).

WHAT WE HOLD

- *Identity data* for each user: email, account profile, behavioral biometric (keystroke timing, edit patterns, pause distributions), generated word + mark + rhythm.
- *Reading data*: answers to six prompts, raw text, derived analytics.
- *Telemetry*: device fingerprint, IP, locale, page events.

WHAT WE DON'T HOLD

- Payment card data (Stripe handles it; we never see card numbers)
- Photographs of faces, voice prints, fingerprints, retina/iris scans
- Customer's source code, proprietary documents, or non-Reading content
- Any data not directly entered by the user during the Reading or Room sessions

ARCHITECTURAL PRIVACY GUARANTEE (THE MOAT)

VEX customers ask: how do we know our leadership can't read individual employee answers?

The answer is structural, not configural:

1. Every Participant's data is keyed to *their* identity, not the employer's.
2. The aggregation worker reads *across rows*, never one row.
3. The leadership view queries an aggregate-only Postgres view that *rejects any query returning fewer than five rows*.
4. *There is no admin role with SELECT permission on the individual rows.* The role does not exist. Granting it would require a database migration and a code deployment by Noctara, both of which we would disclose to the Customer in writing prior to execution.

This is enforced at the database layer (Supabase row-level security) and at the application layer (no service code can express the query that would return individual Reading content to a leadership account).

SUBPROCESSORS (CANONICAL LIST)

| Subprocessor | Role | Location | DPA on file | |—|—|—|—| | Vercel, Inc. | Hosting, edge compute, static delivery | USA | yes | | Supabase Inc. | Postgres, object storage | USA | yes | | Clerk Inc. | SSO, MFA, session management | USA | yes | | Stripe Inc. | PCI-compliant payments | USA | yes | | Resend Inc. | Transactional email | USA | yes | | Anthropic PBC | Claude API (compression, digests) | USA | yes; no training on customer data per Anthropic API terms |

30 days' written notice before adding any new Subprocessor.

ENCRYPTION

- *In transit*: TLS 1.3, HSTS preload, no HTTP fallback.
- *At rest*: AES-256 for database (Supabase managed) and object storage.
- *Application secrets*: held in Vercel env, rotated on key events. No production credentials in source.

AUTHENTICATION

- Primary: Sign in with Google, Microsoft, Apple (SSO via Clerk).
- Backup: magic-link email + 6-digit code.
- Native: behavioral biometric ("type your mark") with email-code fallback when keystroke confidence is low.
- MFA available for VEX administrative accounts.
- No passwords are stored on Noctara infrastructure.

ACCESS CONTROL

- Row-level security enabled on every Postgres table.
- Service-role keys live only in Vercel environment. No production database credentials in source repos.
- Internal access to production data is logged and audited.
- The "leadership read" view is a Postgres view with k-anonymity gate (k≥5).

BACKUP & RECOVERY

- Automated daily backups, 30-day retention.
- Point-in-time recovery available within retention window.
- Disaster recovery RPO 24h, RTO 8h.

LOGGING & MONITORING

- Application logs retained 30 days.
- Access logs (auth events) retained separately for 90 days.
- PII excluded from logs by policy. Stack traces never include user content.
- Anomaly detection on authentication and admin endpoints.

VULNERABILITY MANAGEMENT

- `security\@noctaracorp.com` for responsible disclosure.
- Acknowledgment within 1 business day.
- Patch SLAs follow CVSS severity:
- Critical (9.0.10.0): 24 hours
- High (7.0.8.9): 7 days
- Medium (4.0.6.9): 30 days
- Low (<4.0): next release cycle

BREACH NOTIFICATION

Within 72 hours of confirmed material breach affecting Customer's data. Per DPA Section 9.

COMPLIANCE

- *SOC 2 Type 1 readiness audit complete.* Type 2 attestation in observation window. Letter of engagement available on request.
- *GDPR / UK GDPR*: aligned. Standard Contractual Clauses where applicable.

- *CCPA*: aligned. We do not sell Personal Data.
- *HIPAA*: not in scope. We are not a Business Associate. Customers in healthcare must not transmit PHI through Noctara.
- *PCI*: out of scope. Card data handled by Stripe.

BIOMETRIC LAW

Keystroke dynamics are not voiceprints, faceprints, retina or iris scans, fingerprints, or hand geometry. Most courts reading BIPA, Texas, and Washington biometric statutes find keystroke dynamics fall outside the enumerated categories. We obtain explicit informed consent at the point of every Reading regardless. Pilot terms include Participant-facing consent language pre-approved by counsel.

We do not capture keystroke data outside the Reading or Room sessions. There is no background monitoring.

INCIDENT HISTORY

No reportable security incidents to date. (Updated each quarter.)

PATENT

US provisional patent application 64/048,624 filed 2026-04-24 with Rapacke Law Group. Covers the behavioral-identity-embedded-authentication primitive. Non-provisional filing deadline 2027-04-24.

FOUNDER & CONTACTS

- *Founder & CEO*: Cole Alexander Alkire
- *Address*: 870 Coal Run Road, Marietta, OH 45750
- *Procurement / legal*: legal@noctaracorp.com
- *Security / vulnerabilities*: security@noctaracorp.com
- *Privacy / DPA*: privacy@noctaracorp.com
- *General*: hello@noctaracorp.com

DOCUMENT CONTROL

- This document: `Legal/drafts-2026-05-09/SECURITY-ONE-PAGER.md`
- Counterpart published at: `https://takethemirror.com/trust`
- DPA: `Legal/drafts-2026-05-09/DPA.md`
- MSA (Pilot Light): `Legal/drafts-2026-05-09/MSA-PILOT-LIGHT.md`

COUNSEL REVIEW CHECKLIST

- [ ] Subprocessor list complete and current
- [ ] SOC 2 status accurate (Type 1 readiness vs full attestation language)
- [ ] BIPA section is defensible without overstating
- [ ] HIPAA carve-out is clear
- [ ] Patent application number and dates correct
- [ ] All email aliases routed
- [ ] PDF generation flagged for Phase 4 build (Typst forge-src pipeline)

END OF DOCUMENT . NOCTARA, INC.