HECVAT-Lite — Encephlo Self-Assessment

Vendor: Encephlo Ventures Inc. **Product / Service:** Encephlo B2B Educator Pilot (Educator Studio, Student Web Tutor, Canvas LMS sync, Insights) **Vendor Contact:** Suraj Swaminathan, Founder — Suraj@encephlo.com **Date completed:** August 12, 2026 **Assessment scope:** B2B Educator Pilot (see `security-and-data-flow.md` §1).

> **Note on format.** This document is structured as a HECVAT-Lite-style self-assessment using REN-ISAC HECVAT v3 section ordering. Encephlo has not yet completed an official EDUCAUSE HECVAT submission. All answers below are good-faith and grounded in the source code and infrastructure documented in `security-and-data-flow.md`. Where a control is not yet implemented, the answer says **"No — Gap."** Customers may verify any answer by reviewing the cited file or reaching out to suraj@encephlo.com.

Answer key: Yes · No · Partial · Documented · N/A · Gap

DOCU — Documentation

ID	Question	Response	Notes
DOCU-01	Has the vendor completed a HECVAT for this product?	**Partial**	This HECVAT-Lite is the current self-assessment. Full HECVAT planned 2027.
DOCU-02	Are policies and procedures documented?	**Partial**	`security-and-data-flow.md` and this HECVAT-Lite are in source control. Formal ISMS not yet established.
DOCU-03	Are SOC 2 / ISO 27001 reports available?	**No - Gap**	Pre-revenue startup; SOC 2 Type 1 targeted 2027.
DOCU-04	Is a Data Processing Agreement / FERPA addendum available?	**Yes**	See `dpa-template.md`.
DOCU-05	Is a current subprocessor list available?	**Yes**	See `subprocessors.md`.

COMP — Company Overview

ID	Question	Response	Notes
COMP-01	What is the legal name of the company?	—	Encephlo Ventures Inc.
COMP-02	Where is the company headquartered?	—	United States.
COMP-03	How long has the company been in business?	—	< 2 years (early-stage).
COMP-04	How many employees?	—	Founder-led (very small team).
COMP-05	Is the company financially stable?	**Partial**	Early-stage startup; revenue runway disclosed on request.
COMP-06	Does the company carry cyber liability insurance?	**No - Gap**	Will be procured as a condition of the pilot if the customer requires it.
COMP-07	Are background checks performed on personnel?	**Partial**	Founder is the primary contributor; written confidentiality obligations apply to all contributors.

DOCU / SEC — Application & Service Security (HLAP)

ID	Question	Response	Notes
HLAP-01	Is the application web-based?	**Yes**	Next.js 15 on Firebase App Hosting.
HLAP-02	Are all sessions encrypted in transit (TLS)?	**Yes**	TLS 1.2+ enforced by Google's frontend.
HLAP-03	Are sensitive credentials stored encrypted at rest?	**Yes**	Canvas OAuth refresh tokens / PATs stored server-only with deny-all client rules; encryption at rest by Google (AES-256).

HLAP-04	Is multi-factor authentication available for administrators?	**Partial**	Google Workspace (administrator) supports MFA; Firebase console access via founder's Google account is MFA-protected. End-user MFA at the application layer is on the roadmap.
HLAP-05	Are dependencies tracked and updated?	**Partial**	`npm audit` and Dependabot used; cadence is best-effort, not formally scheduled.
HLAP-06	Is the application protected against OWASP Top 10?	**Partial**	Standard mitigations: TLS-only, Firebase Auth ID-token verification on every callable, parameterized queries (Firestore SDK), CSRF protection on state-changing flows, no `eval` of user input. No formal OWASP audit.
HLAP-07	Is input validated server-side?	**Yes**	Zod schemas validate every callable input.
HLAP-08	Are sessions invalidated on logout?	**Yes**	Firebase Auth ID tokens expire; refresh tokens revoked on logout.
HLAP-09	Are administrative interfaces separated from end-user interfaces?	**Yes**	Firebase / Google Cloud Consoles are separate from the application. No customer-facing admin panel; founder uses Google Cloud Console.
HLAP-10	Is source-code stored in a private repository?	**Yes**	Private GitHub repository.
HLAP-11	Is code review required before merge to production?	**Partial**	Founder-led; informal review for now.

AAAI — Authentication, Authorization, Accounting

ID	Question	Response	Notes
AAAI-01	What identity providers are supported?	—	Firebase Auth: email/password, Google sign-in, Microsoft sign-in. SAML/OIDC against the Institution's IdP available on request (roadmap).
AAAI-02	Are passwords stored using a strong one-way hash?	**Yes**	Firebase Auth uses scrypt-based hashing internally.
AAAI-03	Is account lockout / rate-limiting in place for sign-in?	**Yes**	Firebase Auth applies adaptive throttling and lockout.
AAAI-04	Are sessions time-limited?	**Yes**	Firebase ID tokens expire after 1 hour; refresh-token TTL controlled by Google.
AAAI-05	Is least-privilege enforced for application access?	**Yes**	Firestore Security Rules + Cloud Storage Security Rules enforce per-user/per-educator scoping. See `security-and-data-flow.md` §7.
AAAI-06	Is SSO supported?	**Partial**	Google and Microsoft OIDC sign-in available today; SAML against the Institution's IdP is a roadmap item.
AAAI-07	Are administrative actions logged?	**Yes**	Cloud Audit Logs cover the GCP project.
AAAI-08	Are unused accounts disabled?	**Partial**	Manual today; automatic stale-account disablement is a roadmap item.

BUSI — Business Continuity / DRP

ID	Question	Response	Notes
BUSI-01	Is there a documented business-continuity plan?	**No - Gap**	Reliance on Google Cloud's reliability SLAs. Formal BCP planned 2027.
BUSI-02	RTO / RPO targets?	**Partial**	Inherited from Google Cloud: Firestore PITR within 7 days; Cloud Storage 99.95% availability SLO. Pilot RTO target: 24 hours.
BUSI-03	Are backups tested?	**Partial**	Firestore PITR tested informally; no scheduled drill.

CHAN — Change Management

ID	Question	Response	Notes
CHAN-01	Is there a documented change-management process?	**Partial**	Git-based with branch protection on `main`; feature branches → review → merge → deploy. Formal CAB not in place.
CHAN-02	Are production deploys tracked?	**Yes**	Firebase deployment history + Git history.
CHAN-03	Is there a rollback procedure?	**Yes**	Firebase App Hosting allows traffic redirection to a prior rollout; Cloud Functions can be redeployed from prior commits. Maintained checkpoint branches (e.g., `chore/ai-checkpoint-pre-vertex-ai`) provide known-good revert points.

DATA — Data

ID	Question	Response	Notes
DATA-01	What categories of institutional data are stored?	—	See `security-and-data-flow.md` §3.
DATA-02	Is institutional data segregated by tenant?	**Yes**	Per-educator subtree (`educators/{uid}/...`); Firestore rules + Storage rules enforce isolation; vector chunks and Canvas tokens are server-only.
DATA-03	Is data encrypted at rest?	**Yes**	AES-256 with Google-managed keys (Firestore, Storage, Logging).
DATA-04	Is data encrypted in transit?	**Yes**	TLS 1.2+.
DATA-05	Are customer-managed encryption keys (CMEK) supported?	**No - Gap**	Available on Google Cloud; not enabled by default. Discuss for enterprise tier.
DATA-06	Is data classification documented?	**Yes**	See `security-and-data-flow.md` §3.
DATA-07	What is the data-retention policy?	—	Retained until educator deletion or institutional deletion request; insights cache overwritten on each refresh; logs default 30 days. See `security-and-data-flow.md` §9 and §11.
DATA-08	Is data deletion verified on customer request?	**Yes**	Live data within 30 days, backups within 90 days; written confirmation on request. See `dpa-template.md` §10.

DATA-09	Will customer data be used to train AI models?	**No - never**	Vertex AI per Google's CDPA does not train on Customer Data; Encephlo contractually commits not to in `dpa-template.md` §4.3.
DATA-10	Are instructor-supplied answer keys protected from student disclosure?	**Partial**	Two controls, honestly distinguished. (1) Students cannot retrieve a material marked `answer_key` : enforced in retrieval code (`STUDENT_BLOCKED_MATERIAL_KINDS`), not by a model instruction. (2) The tutor **is** grounded in the key so it teaches the instructor's method; every response is scanned server-side and any value appearing only in the key is blocked before it is sent. This closes verbatim disclosure but **cannot prevent inference from a correct explanation**. See `security-and-data-flow.md` §5.1.

DBAS — Database

ID	Question	Response	Notes
DBAS-01	What database is used?	—	Cloud Firestore (Firestore in Native Mode, multi-region `nam5`). Firebase Storage for files.

DBAS-02	Is direct database access restricted?	**Yes**	No public DB ports; access via Google IAM and Firebase Admin SDK. Application access is mediated by Firestore Security Rules.
DBAS-03	Are queries parameterized / typed?	**Yes**	Firestore SDK enforces typed paths and queries; no SQL injection surface.
DBAS-04	Are database backups taken?	**Yes**	Firestore PITR (7 days) available; full export to Cloud Storage on request.

DCEN — Datacenter / Cloud Hosting

ID	Question	Response	Notes
DCEN-01	Where is institutional data stored geographically?	—	United States. Firestore `nam5` (Iowa + South Carolina). Storage US multi-region. Functions / App Hosting `us-central1` (Iowa).
DCEN-02	Is the hosting provider SOC 2 / ISO 27001 certified?	**Yes**	Google Cloud Platform — multiple certifications; see Google Cloud compliance.
DCEN-03	Are physical-security controls in place?	**Yes**	Google data centers (multi-factor physical access, 24/7 surveillance, etc.).
DCEN-04	Are environmental controls in place?	**Yes**	Google data-center standards.

DRPL — Disaster Recovery Plan

ID	Question	Response	Notes

DRPL-01	Is there a written DR plan?	**No - Gap**	Inherits Google Cloud's regional resilience (Firestore `nam5` is multi-region); formal DR plan planned 2027.
DRPL-02	Are DR drills conducted?	**No - Gap**	Planned 2027.

FIRE — Firewalls / IDS / Network Security

ID	Question	Response	Notes
FIRE-01	Are network-level controls in place?	**Yes**	Inherited from Google Cloud: VPC Service Controls available, default deny-all on Firestore/Storage public access, only HTTPS endpoints exposed.
FIRE-02	Is DDoS protection in place?	**Yes**	Inherited from Google's edge (Cloud Armor / Google Frontend).
FIRE-03	Is there an IDS / IPS?	**Partial**	Google Cloud's built-in detective controls (Security Command Center available). No dedicated IDS today.
FIRE-04	Is logging of network events in place?	**Yes**	Cloud Logging captures HTTPS request logs and Firestore audit logs.

PHYS — Physical Security

ID	Question	Response	Notes
PHYS-01	Where is institutional data physically located?	—	Google data centers in the United States.

PHYS-02	Are physical-access controls in place at the data center?	**Yes**	Google's standards (biometric access, 24/7 surveillance, perimeter security).
PHYS-03	Does the vendor host any infrastructure on-premises?	**No**	All production infrastructure is on Google Cloud.

PPAU — Policies, Procedures, Audits

ID	Question	Response	Notes
PPAU-01	Is a written information-security policy maintained?	**Partial**	This compliance folder is the current artifact set. A formal ISMS is on the 2027 roadmap.
PPAU-02	Is there a privacy policy?	**Yes**	https://encephlo.com/privacy.
PPAU-03	Is third-party penetration testing performed?	**No - Gap**	Internal review only; pen test planned before broad GA.
PPAU-04	Is internal security training performed?	**Partial**	Founder-led; informal.

QASS — Quality Assurance

ID	Question	Response	Notes
QASS-01	Are automated tests in place?	**Partial**	Vitest unit tests for several Cloud Functions and React components; Firestore rules unit tests for B2B paths exist. Coverage is incomplete.
QASS-02	Is there a staging environment?	**Partial**	Branch-based preview deploys via Firebase App Hosting.

SYSM — Systems Management

ID	Question	Response	Notes
SYSM-01	Are systems patched on a defined cadence?	**Partial**	Inherits Google Cloud's managed runtime patching for Cloud Functions / App Hosting / Firestore. Application-level dependency updates are best-effort.
SYSM-02	Are anti-malware controls in place?	**Yes**	Google Cloud's managed runtime.
SYSM-03	Are administrator credentials rotated?	**Partial**	Google account credentials follow Google's security policy (long passphrase + MFA). API keys are being rotated and migrated to Secret Manager — see DATA / VULN gap below.

VULN — Vulnerability Scanning

ID	Question	Response	Notes
VULN-01	Are dependency vulnerabilities scanned?	**Partial**	`npm audit` + GitHub Dependabot alerts.
VULN-02	Is static analysis in place?	**Partial**	TypeScript strict mode, ESLint. Dedicated SAST tooling planned.

VULN-03	Are secrets in source control scanned?	**Partial** — Gap	`.gitignore` excludes `functions/.env`; **`apphosting.yaml` currently contains plaintext API keys for Gemini AI Studio and Google Custom Search.** Mitigation in flight: rotate keys, move to Secret Manager (`secret: SECRET_NAME` references), pre-pilot.
VULN-04	Is there a defined remediation SLA?	**Partial**	Critical: 7 days. High: 30 days. Best-effort.

PRIV — Privacy

ID	Question	Response	Notes
PRIV-01	Is a privacy policy published?	**Yes**	https://encephlo.com/privacy.
PRIV-02	Is institutional / student data sold?	**No - never**	Stated in DPA §4.2 and privacy policy.
PRIV-03	Is data shared for advertising?	**No**	No ad networks, pixels, or first-party tracking cookies.
PRIV-04	Are data subjects' rights honored (access, deletion, correction)?	**Yes**	See `security-and-data-flow.md` §11 and `dpa-template.md` §8.
PRIV-05	Is FERPA addressed?	**Yes**	Encephlo accepts a FERPA "school official" designation. See `dpa-template.md` §2.3 and §12.
PRIV-06	Is COPPA / under-13 handling addressed?	**Yes**	Service intended for users 13+; under-13 data deleted on discovery. See privacy policy §7.

PRIV-07	Is data ever used for AI / model training?	**No - never**	DPA §4.3; Vertex AI per Google's CDPA does not train on Customer Data.

THIR — Third Parties

ID	Question	Response	Notes
THIR-01	Are subprocessors disclosed?	**Yes**	`subprocessors.md`.
THIR-02	Is advance notice given before subprocessor changes?	**Yes**	30 days; see `dpa-template.md` §5.
THIR-03	Are subprocessors contractually bound to equivalent obligations?	**Partial**	Google CDPA, Microsoft DPA, Apple developer terms, Instructure terms, and Resend's DPA are executed standard terms. Inworld AI (text-to-speech, user-initiated only) is used under its published terms without a negotiated DPA today; an institution that prefers no TTS subprocessor can have the feature disabled for its courses.

INCI — Incident Response

ID	Question	Response	Notes
INCI-01	Is a security incident response process defined?	**Partial**	Founder is incident commander; reachable at suraj@encephlo.com. Written runbook in development.

INCI-02	Will the customer be notified of a security incident?	**Yes** — within 72 hours of confirmation	DPA §9.
INCI-03	Will the customer be supported in their own response?	**Yes**	Cooperation commitment in DPA §9.

CLOU — Cloud Services Specific

ID	Question	Response	Notes
CLOU-01	What cloud-service model is in use?	—	SaaS to the customer; PaaS underneath (Firebase).
CLOU-02	Is the cloud provider single-tenant or multi-tenant?	—	Multi-tenant SaaS layered on Google Cloud's multi-tenant infrastructure with Firestore Security Rules enforcing logical tenant isolation.
CLOU-03	Is data co-mingled with other customers?	**Partial**	Logically isolated by tenant in a shared Firestore database; isolation enforced by rules + admin SDK ownership checks. Per-customer dedicated Firebase projects available on request for an enterprise tier.
CLOU-04	Is the cloud provider's compliance documentation available?	**Yes**	https://cloud.google.com/security/compliance

Summary — Key Strengths and Known Gaps

Strengths

- All institutional data stored in U.S. regions (Firestore `nam5`, Storage US multi-region, Functions / App Hosting `us-central1`).
- AI inference is on Vertex AI under Google's CDPA — Customer Data is **not used to train Google's foundation models**.
- Strict tenant isolation enforced by Firestore + Storage Security Rules; Canvas tokens, vector chunks, and roster writes are server-only.
- Insights surface only AI-derived summaries to the educator, never raw transcripts cross-tenant.
- Subprocessor list is short, US-focused, and disclosed in writing.

Known gaps (transparent disclosure)

- Vertex AI uses `global` endpoint (model-availability constraint) — pinning to US once available.
- Embedding path still on AI Studio API — Vertex migration scheduled Q3 2026.
- No SOC 2 / formal HECVAT report yet — 2027 target.
- No third-party pen test yet — pre-GA.
- No SAML SSO yet — available on request.
- Answer-key protection closes verbatim disclosure, not inference (DATA-10).
- Inworld AI (TTS) is used under published terms, not a negotiated DPA (THIR-03).

This HECVAT-Lite is maintained by Encephlo. Material updates to controls will be reflected here within 30 days of effective date.