



SECURITY & COMPLIANCE

Security & Compliance Overview

For executive directors, boards, and auditors — the claim, the controls, and the honest limits.

PREPARED BY

Luminary Impact (SDVOSB)

AUDIENCE

Boards, funders, auditors

CONTACT

support@lilxhub.com

The participant-data and AI protections below are live in our platform and verified by direct test. The organizational-access controls marked "in development" are rolling out — we mark plainly what is live today and what is coming.

Participant data Live today

- **Identity vault:** identifying fields are split off at collection and readable only by your organization's own logins (database-enforced). All working data is coded (P-XXXXX).
- **Intake screening:** every submission and upload is screened server-side for identifying patterns and rejected before storage. Unscreenable file types require your explicit confirmation.
- **Deliverables never name participants** — codes only.

Organizational data

- **Assignment-scoped operator access** **Rolling out** access will narrow to the operator(s) assigned to your work, with administrative overrides flagged, logged, and visible. Today, access to your data is limited to Luminary's own delivery personnel under confidentiality obligations — never offshore staff.
- **Recorded reads** **Rolling out** a metadata record of each read of your briefs — who, what, when, never content — surfaced in your portal. Today your Activity view shows the actions taken on your requests; the read log is rolling out.
- **Strict client isolation** **Live today** your data never informs another client's work.

AI **Live today**

- AI drafts; humans review; delivery to you is a human, gated action — our AI has no send capability.
- No training on your data — contractually committed. AI cannot read the identity vault.

Commitments you can sign

- **Data Processing Agreement:** prohibited uses (no sale, no training, no cross-client use), 72-hour breach notification, deletion within 60 days of exit (backups 90), free export any time.
- **Acceptable Use Policy:** the coded-data rule, in writing, on both of us.
- **AI Disclosure:** exactly what AI touches and never touches. **BAA** available for HIPAA covered entities.

Infrastructure

Supabase (database, encrypted at rest) · Vercel (hosting, TLS) · Stripe (payments — we never hold card numbers) · Resend (transactional email) · Anthropic (AI drafting, no-training API terms) · Dropbox Sign (e-signature) · Netlify (public website). Our full Subprocessor Disclosure is public; additions require 30 days' notice to you.

The honest limits. Our protections are access separation verified by query — not client-held encryption keys. The identity vault is database-enforced (live); operator assignment scoping will be application-enforced with a database backstop (in development). We state which is which, and we don't oversell either.

Contact: support@lilxhub.com · Full detail: the Trust page and our Data Processing Agreement.