Security & Privacy Whitepaper

Catalyst Ed™ · Platform Security Overview · Last updated: May 2026

Architecture

Catalyst Ed runs on a managed Postgres backend with row-level security enforced on every user-scoped table. Role-based access control is governed through a dedicated user_roles table with security-definer functions — never client-evaluated.

Data Handling

Learner artifacts are stored under per-user, per-enrollment paths in private storage buckets. Public buckets are limited to non-sensitive course syllabi. No student-level data is collected by the platform.

Payments

Payment processing is delegated to Stripe and Paystack. Catalyst Ed never stores card numbers, CVVs, or full bank credentials.

Auditability

Authentication events, role grants, certificate issuance, and admin actions are logged with timestamps and actor IDs. SOC 2-aligned controls and rate-limited public forms are in place. A full security review packet is available to districts under NDA.

*This summary is a public-facing overview. The full document is available on request to **info@catalyst-ed.app**.*