DesignTech AI · Security Overview

ARCHITECTURE & DATA FLOW

Your browser
TLS in transit; Auth0-backed sessions; role-based access

→

Application (Render)
Isolated services, private networking, managed TLS, encrypted secrets

→

PostgreSQL (Supabase)
Encryption at rest; Row-Level Security on all tenant data; automated backups + PITR

→

Files & AI (Google Cloud)
Cloud Storage for files; every AI request runs on Vertex AI

TENANT ISOLATION

- Every organization's data is separated at the database with **PostgreSQL Row-Level Security**, enforced on every query.
- Organization scoping is applied in the application and storage layers as well.
- Isolation is verified by an **automated check in our build pipeline**.
- Your sources never cross into another tenant; your content powers your workspace only.

AI PROCESSING PATH

- AI requests go **directly to Google Vertex AI** with no third-party routing intermediary.
- Enterprise model services do **not use your prompts or content to train** their models.
- Execution logs are short-lived and redacted for secrets.
- Everything produced in your workspace is **yours** to use, publish, edit, and keep.

IDENTITY & ACCESS

- Authentication is handled by **Auth0 by Okta**.
- Access is role-based: super admin, organization admin, or member, with permissions scoped to the organization.
- Outbound/publishing actions wait for explicit user approval.

OUR COMPLIANCE ROADMAP

- **SOC 2 Type I:** on our roadmap; the target date publishes at designtech.ai/trust when the audit is scheduled.
- **Penetration test:** independent testing planned; status publishes when engaged.
- **Data Processing Agreement:** available now, on request.

SUBPROCESSORS

PROVIDER	ROLE	KEY CERTIFICATIONS (PROVIDER-HELD)
Render	Application hosting	SOC 2 Type II, SOC 3, GDPR DPA
Supabase	Managed PostgreSQL	SOC 2 Type II, ISO 27001, HIPAA, PCI DSS
Google Cloud	File storage & Vertex AI	SOC 1/2/3, ISO 27001/27017/27018/27701, PCI DSS, HIPAA, FedRAMP High
Auth0 by Okta	Identity & authentication	SOC 2 Type II, ISO 27001/27017/27018, PCI DSS, HIPAA, CSA STAR