

Security overview and questionnaire answers

Trustfield - <https://trustfield.dev>

Generated 2026-10-25 - written for enterprise buyers

This document answers the questions a security reviewer, lawyer or platform team usually asks. It describes mechanisms that are live today. We do not claim SOC 2, ISO 27001 or an external audit, and we will say so rather than invent a certificate.

What does Trustfield do?

It performs an external, read-only security review of a public web app and produces a report: leaked keys in the client bundle, open database rules, unverified payment webhooks, missing headers, exposed files, dependency CVEs (repo scans) and AI prompt-injection exposure. It is not a penetration test and not a security certification.

Do you access our database, source code or user data?

No. Scans read public pages and headers only. A GitHub scan requires you to attach a public repo; we download a read-only archive, analyse it, and do not keep the source. We never ask for database credentials or model API keys.

Where is data stored and for how long?

Reports are stored in Supabase (United States) for 30 days after the scan, then deleted. Email addresses are kept until you ask us to delete them. Anonymous aggregate statistics (no target, no email) may be kept to publish issue trends. Rate-limit data is kept for a few hours.

Who are your subprocessors?

Render (hosting, US), Supabase (report storage, US), Cloudflare (DNS/TLS/proxy, global edge), Razorpay (payments, India), Resend (transactional email, US), Hostinger (domain and mailbox, EU), and Ahrefs (cookieless aggregate analytics). Full table: /subprocessors. A DPA is available on request.

How is payment data handled?

Payments run through Razorpay's hosted checkout. Card details are entered on Razorpay's page and never touch Trustfield servers. Webhooks are verified with HMAC-SHA256 signatures, and the expected amount, currency and report id are checked before a report is unlocked.

Do you use AI, and is our data used for training?

The report copilot (Ask about this report) sends the report text and your question to DeepSeek's API to generate an answer. We do not train models on customer data and we do not send your source code or database. The copilot is optional for buyers.

What security controls are in place?

TLS everywhere with HSTS (max-age 31536000, includeSubDomains); CSP that only allows our own scripts and the analytics origin; X-Frame-Options DENY; nosniff; Referrer-Policy; Permissions-Policy; no advertising cookies; admin access behind a long random token; rate limits per IP; SSRF protection blocks private IPs and re-checks redirects. We do not claim SOC 2, ISO 27001 or a third-party audit.

Can you sign an NDA or DPA?

Yes to an NDA by email. A data-processing addendum is available on request for business customers; write to the contact address and we will send the current template for review. We are a sole proprietorship in India; we will not pretend to be a larger entity.

How do we delete our data?

Use /delete-account or email us with the report link. We delete the report, the stored email and related records within 7 days and confirm by email. Reports also auto-delete 30 days after the scan.

What happens after a payment if the report does not arrive?

Email us with the payment id. We re-run the scan or refund the full amount within 7 days. If a finding is factually wrong, we fix the check, add a regression test, and refund that report. Policy: /refund.

Do you have a vulnerability disclosure programme?

Yes. Email the contact address with 'security report' in the subject and steps to reproduce. We acknowledge within 2 business days and will not pursue legal action for good-faith testing limited to your own account and data. Details: /security.

What is your uptime and SLA?

There is no SLA. The service runs on a small stack and is best-effort; the public /status page lists known incidents honestly. The free tier can cold-start in under a minute; paid reports are stored so they remain available after restarts.

Is scanning a third party allowed?

No. The requester must confirm they own the app or have explicit permission. We rate-limit scans, never run exploitation, and block private-network targets. Our scanner identifies itself and offers an opt-out page at /bot.

Which compliance frameworks do you follow?

We apply data-minimisation and deletion principles consistent with India's DPDP Act and GDPR, but we are not certified under either and we do not claim 'compliance'. Enterprise questionnaires that require a certificate should be answered by your own auditor.

Can we get the report for a client handover?

Yes. The agency pack gives ten client-ready reports; each report can carry 'Prepared for <client> - handover by <agency>'. See /agency. Same scope and limits as the standard report.

How do we contact you?

Email the address on every page. A real person answers, usually within one business day. The operator is Dhruv Kumar, Faridabad, India (sole proprietorship), named in /about and /terms.
