Security answers

Short answers for a security or IT review of Crossruled during free early access. Each one describes the product as it runs on the date above, including where the answer is no. The longer version is crossruled.com/trust. Questions go to security@crossruled.com.

Hosting and data	
Hosting	The app runs on Vercel, on the hosting plan we use during early access, which is not its Pro or Enterprise plan. Data is in Google Cloud Firestore and sign-in is Firebase Authentication, on Firebase's no-cost plan.
Data region	Firestore multi-region nam5, in the United States. There is no India or EU region today.
What to upload	Demo data only during early access. Do not upload real employee data until we tell you the hosting plan is ready for it. Vercel's data-processing terms apply to its Pro and Enterprise plans, not to the hosting plan we use during early access.
Tenant isolation	Each firm is its own tenant. Firestore security rules check the signed-in user's profile, tenant and role on every read and write. A rules test suite, one of whose tests is a user of another firm being refused your data, runs on every push to the main branch.
Encryption	In transit: HTTPS only, with HSTS for two years, set by our host. At rest: Google Cloud's default encryption for Firestore and Firebase Authentication. No customer-managed keys. Backup copies sit on a FileVault-encrypted computer.

Access	
Roles	Six: owner, admin, finance, HR, delivery and viewer. Per-person cost, role salary bands, proposal prices and the audit log are readable by owner, admin, finance and HR only, and the rule is enforced in the database. Delivery and viewer logins never see pay. Bill rates are visible to every role.
Sign-up and passwords	By invitation only: a one-use access code bound to one email address. Passwords are 12 to 128 characters with a lowercase letter and a digit. A password is set only by its owner, through a reset email; no one at Crossruled sets a customer's password.
Multi-factor authentication	**No.** Sign-in is email and password only.
Single sign-on (SAML, Microsoft or Google)	**No.** Microsoft and Google sign-in, SAML and SCIM are roadmap items with no date yet.
Removing a user	Removing a user, or setting the account inactive, cuts access at once. A sign-in token on its own grants nothing.
Operator access	Crossruled is one person. Only the operator, Rajan Agarwal, can reach workspace content, through Google Cloud credentials used for backups and on a written support request. The operator console shows no workspace content. There are no other staff with access.

Incidents	
Reporting	Write to security@crossruled.com. A suspected exposure across tenants is severity 1 and is handled first. The steps are on crossruled.com/incident.
Notice to you	If workspace content is accessed without authority or lost, the workspace owner is told by email within 24 hours of our becoming aware, with what we found and what we changed.

Operations

Backups	Manual. The operator exports the database to a FileVault-encrypted computer in India to test that restores work, and deletes each copy by hand within 30 days of making it. Restores have been proven on the emulator only. The no-cost Firebase plan has no managed or point-in-time backup.
Audit log	Every change to people, roles, projects, allocations, proposals and costs writes an entry: the user's email, the action, the record, the time and, for most records, the values before and after. Per-person cost values are never written into it. Entries are written by the app in the browser as each change saves, so a modified client could skip its own entry. No one in the workspace can edit or delete an entry. A server-written audit trail is a roadmap item.
Logs	Our hosting plan keeps runtime logs for one hour. There is no long-term store of request logs today.
Uptime	No uptime SLA and no third-party status monitor during early access. A public health endpoint reports the build and configuration state.
Web headers	A Content-Security-Policy with a per-request nonce, X-Frame-Options DENY, nosniff, a strict Referrer-Policy and a Permissions-Policy, on every page.
Dependencies	npm audit at the critical tier, the unit tests, the rules tests and the build run on every push to the main branch.

Assurance

Penetration test	**No.** No third-party penetration test has been done. A read-only, AI-assisted review of the code, rules and live headers ran on 29 September 2026, with re-verification through 30 September; its two high findings were closed before that release. The records are available on request.
SOC 2 or ISO 27001	**No.** Crossruled holds no SOC 2 report and no ISO 27001 certificate. Both are roadmap items.

Data lifecycle

Subprocessors	Google LLC: Firebase Authentication and Cloud Firestore, nam5, United States. Vercel Inc.: hosting, serverless functions and logs, United States. Email to crossruled.com mailboxes is held by Zoho Corporation as correspondence, not workspace content. Owners get 14 days' notice before a subprocessor is added or replaced, and may leave.
Retention	The trial runs 14 days; for a pilot firm we extend it to cover the four-week pilot on the day the workspace opens, and further on request. If no one asks us to keep or delete a workspace, we email the owner and delete it 90 days after the evaluation ended, with at least 14 days' notice.
Deletion on request	Within 30 days of a written request from the owner, backup copies included.
Export	Any day, from Settings: a JSON file of people, roles, projects, allocations and proposals, and the reports as CSV. The audit log is not in the export.

Who you are dealing with

Operator	Rajan Agarwal, Delhi, India, an individual who runs Crossruled as a trade name. No company is incorporated yet. The terms, the DPA and the privacy notice name him as operator.
Documents	crossruled.com/trust, /dpa, /privacy, /terms and /incident. The DPA is part of the terms; there is no separately signed DPA during early access.