Jilu

Security at Jilu

The commitments on Jilu's security page, on one page.

ONE-PAGER · JILU.SH/LIBRARY

Jilu holds the record of how a company works, so its safeguards matter more. Every control below carries the state the security page gives it: Designed means the control is specified in the locked architecture and stated as a commitment; Planned means Jilu has committed to it and has not built it yet.

01 · Protect the data

Workspaces kept apart [Designed] — each workspace's data is sealed off from the others in the shared Postgres database, and every search runs under that workspace's own rules.

Encryption in transit and at rest [Designed] — data is encrypted as it moves between the customer's tools and Jilu, and as it sits in Jilu's stores; keys stay separate from the data they protect.

Separate keys for each workspace [Planned] — on the roadmap, so one workspace's key never unlocks another workspace's record; not shipped yet.

You choose what Jilu collects [Designed] — the customer decides which channels, spaces and kinds of data Jilu collects; direct messages and HR spaces stay out unless the customer deliberately includes them.

02 · Control access

SSO and MFA through your identity provider [Designed] — people sign in through the customer's provider, with MFA enforced under the customer's own policy. Available on Business and Enterprise.

SCIM [Designed] — accounts are created and removed automatically with the identity provider account, so a leaver's access ends with the account that gave it. Available on Enterprise.

Separate admin roles [Designed] — each role holds only the access its work needs; changing what Jilu collects is an admin action, logged and shown to the customer.

No standing staff access [Designed] — no one at Jilu can read customer data by default; support access is granted only for a named reason, for a limited time, after the workspace admin approves it, and each grant is logged for the customer to see.

03 · Detect and respond

An audit log that cannot be rewritten [Designed] — every read is logged, by a person or the agent; the log only grows, each entry carries a fingerprint of the entry before it, and the latest fingerprint is stored outside the database hourly and checked daily.

Logs you can take with you [Designed] — logs are exportable into the customer's own monitoring. The customer-visible audit log is included on Business and Enterprise.

Incident response, in the contract [Designed] — the data processing agreement will carry the commitment: Jilu will notify a customer within 48 hours of confirming an incident that touches that customer's data.

Outside security testing [Planned] — Jilu commits to an independent security test every year once the service is running; until the first test runs, this stays listed as a commitment.

04 · Prove it

Evidence on request [Planned] — the review pack is in preparation; on request today a reviewer can receive the security programme summary and the certification roadmap. The data processing agreement and the sub-processor list are not final documents yet.

Exit [Designed] — a customer can stop Jilu collecting, export the full record in open formats, and have its live data and everything built from it deleted; backups are emptied within 35 days.

Status today [Designed] — Jilu holds no SOC 2 or ISO 27001 certification today, and claims none. The year-one plan is SOC 2 Type I; SOC 2 Type II, then ISO 27001, follow after year one. Dates on the roadmap are plans.

Drawn from the security page at jilu.sh/security, where each commitment stands in full.