

Template draft. This is standard boilerplate prepared for review. It is not legal advice. Replace every [highlighted placeholder], confirm each statement matches how IdeaLine actually operates, have a qualified lawyer review it for your jurisdictions, and delete this notice before publishing.

Security Statement

Last updated [EFFECTIVE DATE]

Your team's plans, ideas and files are your business. This page says plainly how IdeaLine protects them, what we do not yet have, and how to reach us about a security concern. We only list measures that are actually in place.

1. Who can get in

- **Invitation only.** Nobody can create an account on their own. The database refuses sign-ups from any email address that has not been approved.
- **Separate workspaces.** Row-level security in the database keeps each workspace invisible to every other, enforced by the database and not only by the app.
- **Roles and permissions.** Admin, Editor, Contributor, Member and Visitor roles, plus a permission level and a view limit for each person. The database enforces the read-only and admin-only boundaries.
- **Passwords and sign-in links** are handled by our authentication provider. We never see or store your password. Sessions end after a period of inactivity.

2. How data is protected

- Traffic between your browser and IdeaLine uses HTTPS (TLS), and browsers are told to use HTTPS only.
- Data is encrypted at rest by our infrastructure providers.
- We store links to your files, never the files themselves, so documents keep their original permissions.
- Share links store only a hash of the token, can expire, and can be revoked.
- The activity log is append-only: the application cannot edit or delete entries.
- Strict browser security headers (content security policy, frame blocking, no sniffing) are set on every page.
- Our server-side secrets are kept in the hosting provider's encrypted environment settings and never in code or in the browser.

3. Your data stays yours

You can download everything at any time (migration pack, Excel or JSON), schedule backup emails, delete a person's access immediately, and delete your account or workspace yourself. See the [Data Policy](#) for retention: 6 months of activity history on Starter, 12 months on Team and for as long as the account exists on Studio.

4. Providers we rely on

Provider	What it does for IdeaLine
Supabase	Database, authentication and live updates
Vercel	Hosts the website and application and runs our server functions
Resend	Sends transactional email such as invitations, password resets and backups
Cloudflare	Domain name and DNS
Google Analytics	Optional website analytics, only if you accept (never inside the application)

Backups and recovery

We take a full, encrypted backup of the database and the sign-in account list **every hour, on the hour**, and store it with a different provider from the one that hosts the database. Hourly copies are kept for 35 days and daily copies for 90 days. Each backup is verified after it is written and a failure alerts our team. Website deployments can be rolled back instantly to any earlier version. Details are in the [Data Policy](#). [Confirm live before publishing]

Payments

Card details are entered only on Stripe-hosted pages and never reach IdeaLine. Stripe is certified to PCI DSS Level 1. See the [Payment Terms](#) and [Stripe: PCI compliance guide](#).

5. Where we are on formal certification

IdeaLine is **not yet** independently certified (for example SOC 2 or ISO 27001). We are building to the same controls: least-privilege access, an audit trail, change review, encryption, vendor

review, backups and an incident process. We will publish a report here when an independent audit is complete, and we will not claim a certification we do not hold.

6. Reporting a vulnerability

If you believe you have found a security issue, email [SECURITY EMAIL, e.g. security@idealine.io]. Please include what you found and how to reproduce it, and give us reasonable time to fix it before sharing it publicly. We will acknowledge reports within [3] business days, keep you informed, and will not take legal action against good-faith research that avoids other people's data. Our [security.txt](#) has the same details.

7. If something goes wrong

If an incident affects your data, we will tell affected customers without undue delay, explain what happened and what to do, and meet any legal notice deadline that applies to us.