FAQ: Security and data protection

From the SourceLace manual: How SourceLace limits access, protects what it keeps, separates organizations, and keeps chosen fields away from the AI.

SourceLace version 0.1.0 · Made November 22, 2026
The latest version is at https://sourcelace.ai/docs

Security and data protection

How SourceLace limits access, protects what it keeps, separates organizations, and keeps chosen fields away from the AI.

How does SourceLace keep people to their own access?

Each person connects most systems with their own login, so each system's own permissions, roles and sharing rules decide what they see and change. SourceLace adds its own limits on top, such as access by group and data protection rules, and never removes any.

Details: Access control.

Does Search everything copy or index our systems?

No. Search everything asks each system at the moment someone searches, with that system's own search and the person's own access, so results always follow each system's current permissions. SourceLace builds no index and keeps no copy: the results are held only like any other answer, for 30 minutes at most, and then deleted. Data protection rules apply to every result, and each system searched is recorded in the audit trail, without the results themselves.

Details: Why nothing is copied.

Is our data encrypted?

Yes. Everything travels over HTTPS or TLS, and SourceLace checks your systems' certificates. What SourceLace keeps for your organization that could be sensitive (people's sign-ins to your systems, secrets, saved chats, AI agents' data and held results) is encrypted with keys per organization.

Details: Encryption.

Can we bring our own encryption key?

Not yet. Each organization's data is already encrypted with its own key. You can bring your own AI key.

Details: Encryption.

Is our data separated from other organizations?

Yes. Everything SourceLace keeps is tied to your organization, every request is checked against the signed-in person's organization, and each organization's sensitive data is encrypted with its own key. An email address belongs to one organization only.

Details: Is customer data separated between organizations?.

Can SourceLace staff see our data?

SourceLace's staff manage your account (plan, admins, contract and single sign-on). What they see never includes data from your systems, sign-ins to them, secrets or AI keys, and every change they make to your organization is recorded in your own audit trail under their name. Admins see those entries on their own with **SourceLace staff** on the **Audit log** page.

Details: Can SourceLace staff see our data?.

What happens to the secrets and keys we enter?

They are encrypted with your organization's key as soon as they are saved. They are never shown again, never returned by any interface, and never written to a log, the audit trail or a support bundle. To change one, type a new one.

Details: Keys: who brings each one, and where it is kept.

Can we hide or mask fields from the AI?

Yes, on every plan. On the **Data protection** page an admin hides fields, masks values such as email addresses, phone numbers, US Social Security numbers, card numbers and IBANs, or adds their own patterns. The AI gets placeholders instead of the values. People who are allowed still see the real values in the SourceLace app, and changes are made with the real values.

Details: Data protection.

Do the data protection rules apply everywhere?

Yes. They apply to the assistant in the SourceLace app, AI agents, SourceLace Runners and people's own AI apps alike. Masking has limits: it cannot cover what someone can work out from other information, what someone types into their own AI app (in the SourceLace chat the detectors and your patterns also check the question you type), or text inside images and scans. The manual lists what is not covered.

Details: What is not covered.

Can SourceLace be tricked into running a harmful query?

Every query is checked before it is sent: one read-only request in the system's own language, with anything that writes, deletes or runs code refused. Data that comes back from your systems is treated as data, never as instructions.

Details: How queries stay read-only.

How do we report a security issue?

Email security@sourcelace.com. There is no bug bounty programme yet.

Details: Vulnerability management and secure development.

Is it safe to add a vendor's MCP connection?

SourceLace applies its own rules to it. Each person signs in to the vendor with their own account, or the source is clearly labelled as a shared account. Only the tools your admin allows can be used, every call is audited, your data protection rules apply to what comes back, and anything the vendor sends (tool names, descriptions, answers) is treated as data, never as instructions. Calls go only to public https addresses, never to internal networks. What the vendor does with each request is governed by your agreement with that vendor.

Details: Safety and What to know before you add one.

Where can our security reviewers get more detail?

Start with Security and privacy and Security questions, which answer most questionnaires one by one. Deeper detail, such as how SourceLace is built and run, is in a security review pack that we share under NDA. Ask security@sourcelace.com.

Details: What can we request for a security review?.

How is SourceLace's hosting protected?

SourceLace runs in a private network in the United States: its database cannot be reached from the internet, a web application firewall blocks common attacks, and connections use TLS 1.2 or later. Threat detection runs all the time, every administrative action is recorded, and only a few named staff can reach the environment, through single sign-on with multi-factor authentication.

Details: How is the hosting environment protected?.

What does "shown to you only" mean in an answer?

When your admin masks a field, the AI only works with a placeholder. If you are allowed to see the real value, SourceLace puts it into the written reply on your screen and marks it with a small highlight and the words "shown to you only". The AI never had that value, and other people who open the same chat but are not allowed to see it get the placeholder. Copy the text with care: the value goes with it.

Details: Real values for the right people.