Ask Lou — Security Overview

Prior Solutions LLC · Version 2.2 · 24 October 2026

Audience: prospective and current customers, and their security reviewers. This document describes the controls protecting your financial data in Ask Lou. It is written in plain language and deliberately omits internal implementation detail. For control-level detail mapped to SOC 2 criteria, request our System Description under NDA.

Ask Lou is in Closed Beta. We are building to SOC 2 criteria (Security, Availability, Confidentiality and Processing Integrity) and are not yet audited or certified. Where a control is partial or planned, this document says so. Section 14 lists what we know is incomplete.

1. What Ask Lou holds

Ask Lou is a fractional-CFO platform. When you use it, we hold:

- Your chart of accounts and trial balance data, imported by upload or from your QuickBooks company with your authorization
- Derived financial statements: balance sheet, income statement, cash flow, KPIs
- Fixed asset and debt schedules you enter or import
- Conversations with Lou, our AI assistant, which reference the figures above
- Account information for your users: name, email, phone, company membership
- Files you upload: import source files, loan documents, company logos, support screenshots and attachments

We do not hold payment card numbers; billing, when it starts, is processed by our payment provider on its own systems.

We do not modify your accounting system. Imports are one-way: we read from your books and build our own mapping on top. Corrections made inside Ask Lou change our mapping, never your source ledger.

2. Authentication

Identity is managed by Clerk, a specialist authentication provider. We do not store or handle your users' passwords.

Every request that reaches customer data carries a verified session, checked where the data is accessed (each page, each operation), not at a routing layer, so a request cannot reach protected data by taking an unexpected path through the application. A build check fails any change that adds a page or operation without a session check.

2.1 Multi-factor authentication

Multi-factor authentication is required for every user, with no exception for our own staff. A user who has not completed enrollment is not treated as signed in. Supported second factors: authenticator apps (time-based codes), passkeys (phishing-resistant), and single-use backup codes for recovery.

Recovery is a written procedure, not a favor. A second factor is removed only after identity is verified through a channel the requester did not choose; accounts with elevated access need two forms of verification, one a live video call, and a second approver. Every recovery is recorded.

2.2 Additional sign-in protections

- Device Trust: sign-ins from an unrecognized device need additional verification.
- Breached-password rejection at sign-up, sign-in and password change.
- Password strength enforcement, with a 15-character minimum.
- Lockout after repeated failed sign-ins.
- Bot protection on sign-up.
- User enumeration protection: the system doesn't reveal whether an email address has an account.

3. Authorization and tenant isolation

Your data is isolated from every other customer's by an authorization check on each data operation, not by a network or database boundary alone.

Every operation is built from a small set of typed access patterns, each carrying its own authorization rule: a valid session, a session resolved to your account, or verified access to a specific company. The company being accessed is resolved from your verified session and your stored grant, never from a value supplied by the browser. This is the most important control we operate.

Records named in a request are checked against your company too. Where an operation names a specific record (an account mapping, a document, a file), the application confirms it belongs to the company you are working in before using it.

No operation is reachable without a session except our marketing pages' deliberately public, rate-limited endpoints, which read no customer data.

User roles within your company

Role	Can
Owner	Full access, including billing and user management
Admin	Full data access and most management functions
Member	Read and write financial data
Viewer	Read only

You can also define custom roles with per-permission grants. An unrecognized role falls back to viewer: least privilege on the failure path. The primary owner of a company can't be removed or demoted by another user.

4. Our staff's access to your data

Internal role	Purpose	Access to your screens
Support agent	Front-line ticket handling	Read-only
Support lead	Escalation and team management	Read-only
Super admin	Engineering and administration	Read and write

Support staff viewing your company are blocked from making any change, enforced at the data-access layer rather than by each screen.

Every staff access to a customer company is written to an audit log with the staff member, the company, the action, the time, the IP address and the browser, and flagged as sensitive data access. Our internal console is gated on the server, and every internal page checks its own permission.

Who has access is reviewed every quarter: every staff account in Ask Lou and in each provider we use, each decided keep, change or remove, nobody deciding their own access, with the evidence kept.

5. Encryption and file storage

- In transit: all traffic is served over HTTPS/TLS.
- At rest: customer data is encrypted at rest by our providers (database, file storage, identity). Each provider's security assurance (its SOC 2 report or equivalent) is reviewed yearly.

Uploaded files are held in private storage, and every read is access-checked. A private file has no address that works on its own; every file is served through the application, which re-checks on every request that the person asking may see it. Uploads are checked by their content, not the name or type the browser declares.

Company logos are the one exception, by decision: they are meant to be displayed on screen and in exported statements, contain nothing sensitive, and are held in public storage. Logo uploads refuse file types that can carry script.

6. AI and your financial data

AI is off by default and enabled per company. No AI feature can reach a company's data unless that company has enabled it; the check fails closed.

Lou cannot choose what to read. Lou can call only a fixed, named allowlist of read operations; anything outside it is refused by the application, not by instruction. The company whose data those operations return is supplied by the application from your verified session, never chosen by the model.

Lou never calculates your numbers. Every figure Lou reports is returned by the same calculation code that

Changes to your data need your explicit approval. When Lou proposes a change, he shows exactly what would change, row by row; nothing is applied until you approve. At approval your identity and permissions are re-verified, and every change confirms the record belongs to your company before writing. Proposals expire after five minutes; every proposal, approval, rejection and failure is recorded. One narrow exception: notes you ask Lou to write on an account or period are written directly, after he confirms the wording with you.

One AI provider: Anthropic. Every AI feature in Ask Lou uses Anthropic's commercial API, enforced in the application: if our model configuration were ever set to another provider, that setting is ignored, and a feature fails rather than send data elsewhere. Adding a provider would be a deliberate change, announced here first.

What is sent: your question, the recent conversation, documentation about the page you're on, and the financial context needed to answer, including figures on your screen, the results of Lou's lookups, your company name, and notes on the accounts in view.

- Training. Under Anthropic's commercial terms, your data is not used to train their models.
- Retention at the provider. Anthropic keeps API inputs and outputs briefly for abuse monitoring, then deletes them automatically.
- Prompt caching. We use Anthropic's short-lived prompt caching to reduce cost and latency; the cached part includes your company name and on-screen context.
- Zero retention. We do not currently hold a zero-retention agreement with Anthropic.

Conversation retention. Chat histories are purged once a conversation has had no activity for 90 days, by a daily job that records evidence of each purge.

Abuse controls. AI requests are rate-limited per account. Customer-written text that enters Lou's instructions (account names, notes, labels, your company name) passes through a sanitizer that strips known prompt-injection patterns, and Lou's instructions treat it as data, not instructions. Likely injection attempts are logged.

All AI use is logged with the provider, model, token counts, duration and outcome.

7. Logging, monitoring and review

- Administrative actions are audit-logged with who, what, when, IP and browser. Audit writes for actions touching customer data are part of the same transaction: if the record can't be written, the change doesn't happen. Every view of a compliance evidence file is recorded too.
- Application errors are captured with severity and tracked to resolution. Error records never contain the text of your conversations with Lou.
- Scheduled jobs write a structured run record, shown on an internal health dashboard; failures raise an alert to named staff.

- Automated control checks run daily against our own controls (multi-factor coverage, code review and release approval, audit-log activity, retention jobs, backup confirmations, provider assurance, training, device attestations and more), and record each result as compliance evidence. No AI is used in any check.
- Our leadership reviews what needs attention every week, and meets quarterly on security, risks, incidents and access, with each review recorded.

Machine-to-machine endpoints (scheduled jobs, build callbacks, inbound webhooks) authenticate with a secret compared in constant time or with the sender's signature. There is no development bypass, and a missing secret causes a rejection rather than an open endpoint.

8. Data retention and deletion

Data	Retention
Lou conversation history	90 days after the conversation's last activity
Records of the topics you ask Lou about	90 days after a topic was last asked
AI usage records (model, tokens, timing; no conversation text)	90 days
Application error records	180 days; records linked to a support ticket keep the link, with request detail removed at 180 days
Administrative audit log	2 years
Financial data you import	The life of your account; returned or destroyed on request
Demo booking details	24 months after the meeting, unless linked to an account
Personal data in an outbound email record	13 months, then removed
Email delivery events	13 months

Retention runs automatically and records evidence of each run. One legal-hold setting pauses every purge while records must be kept.

On termination, a company's data is anonymized by default, or deleted in full on request.

9. Change management

Every change reaches production through a pull request, reviewed by someone other than its author and tested by someone other than its author on our test site before release; who reviewed and who approved is recorded for every change. Automated validation (lint, a production build, the test suite) must pass first. Database changes are additive, applied by a logged script, and recorded in that database's change log; emergencies take a documented hotfix path.

No automated pipeline writes application code. A pipeline that generated code was assessed as incompatible with these controls and removed in September 2026 (its code and records deleted), as was an AI test writer in October 2026. Our developers may use AI coding assistants; what those produce goes through the same review

10. Subprocessors

Our current subprocessors, and the customer data each one receives, are listed at ask-lou.com/legal/subprocessors (https://ask-lou.com/legal/subprocessors). That list is generated from our provider register, the system of record, so it is always current.

Services you connect with your own account, such as QuickBooks, are listed there separately. Our payment provider will be added before billing starts. Tools we use internally that receive no customer data (source control, our password vault, office software, our domain registrar) are on our provider register but not on the public list.

Every provider is approved before it receives customer data, and each critical provider's security assurance is reviewed yearly.

11. Vulnerability and dependency management

Dependencies are reviewed weekly under a written procedure owned by our CTO: the production dependency audit is kept at zero known vulnerabilities, and install scripts run only for an approved list of packages. Fixes are prioritized by risk (authentication, payments, the application framework, and anything that processes uploaded files first). A Content Security Policy limits the scripts our pages can run, and violations are reviewed weekly.

12. Accessibility

Ask Lou has not yet been assessed for accessibility conformance. We have not run a WCAG audit, and make no Section 508, ADA or WCAG conformance claim. Planned before general availability: an automated accessibility pass, manual keyboard and screen-reader testing of the financial statement pages and main workflows, and fixing what they find. We will state a conformance level when we have tested for one.

13. Incident response and recovery

Incidents are handled under a written Incident Response procedure: reported within an hour of detection, contained within four hours, affected customers told without undue delay and within 72 hours of confirming an incident affecting their data, and closed with a written root cause and the changes made. Every incident keeps a timeline of each action and when it happened. We rehearse the procedure with a tabletop exercise every year. To date, no data breach has been observed or suspected.

Backup and recovery. Our database is backed up every 12 hours (kept 2 days) and every 24 hours (kept 30 days); we confirm both schedules every month. Our recovery point objective is 12 hours (the most data a restore could lose) and our recovery time objective is 8 hours (from the decision to restore to the service back with checked data). We have not yet run our first timed restore test; it is scheduled before Open Beta, and yearly after. We don't describe backups that have never been restored as a recovery capability, and this section will give the date and result of our most recent test once it exists.

14. Where we are, honestly

Known gaps, in our own priority order:

- First restore test not yet run (section 13); scheduled before Open Beta.
- Accessibility not assessed (section 12).

Closed since version 1.2: a written incident response procedure with a 72-hour customer notification commitment; stated recovery objectives and monthly backup confirmation; weekly dependency reviews with a named owner; every change's reviewer and approver recorded; quarterly access reviews completed with evidence; every operation now needs a session (the unclassified endpoints are gone); permission checks on every internal staff page; a single AI provider, enforced for every feature.

15. Compliance status

Ask Lou is being built to SOC 2 criteria, and we are not yet audited or certified. We say so plainly.

What exists: written, versioned policies (Data Protection and Security, AI Usage, Engineering Security Standard, Recovery Plan), approved by leadership and acknowledged by every team member in the app; a risk register assessed yearly; security training with a pass mark, yearly; yearly attestation of every work device; a provider register with yearly assurance reviews; quarterly access reviews; a catalog of 49 controls mapped to the criteria, 24 of them checked automatically every day; written procedures for incidents, customer data issues, releases and more; weekly and quarterly reviews; and a System Description. Our compliance program formally starts with our production release, when the first cycle of each of these is completed.

Customers with a compliance requirement can request our System Description under NDA.

16. Contact

Security questions, vulnerability reports and questionnaire requests: ben@priorsolutionsllc.com

We welcome vulnerability reports and will acknowledge them. We do not currently run a paid bounty program.

Product support:

- General questions: the contact form on our marketing site
- Demo requests: the scheduling form on our marketing site
- Company contact form, in Company Settings
- Ticket system, inside Ask Lou: captures a screenshot, severity, type, description and attachments; you can track progress, comment, and reopen or close a ticket

This document is maintained by Prior Solutions LLC. Material changes are reflected in the version number above. Every claim here is intended to correspond to a control that exists and can be evidenced; if you find one that doesn't, tell us and we'll correct it.

Document history

Version	Date	Change
1.2	29 September 2026	Private file storage; content-checked uploads; retention windows for every store of customer-derived data.
2.0	23 October 2026	Rewritten from the SOC 2 program: incident response and its 72-hour commitment; recovery objectives; one AI provider enforced for every feature; reviewed and approved changes; quarterly access reviews; weekly dependency reviews; no session-less operations; updated retention, subprocessors and gaps.
2.1	24 October 2026	Published at ask-lou.com/security. Passages marked internal stay in this file for the copy shared on request and are left off the published page and PDF. Closed Beta; AI rate limiting stated as per account; one security contact.
2.2	24 October 2026	Section 10 links to the published Subprocessors page, generated from the provider register, in place of its own copy of the list.