

Security & Trust at Aventide

How we protect your business data, in plain language.

Last updated October 17, 2026

SOC 2 Type 2 infrastructure

Vercel, Supabase, Anthropic and Cloudflare each publish an independent SOC 2 Type 2 report.

PCI DSS compliant payments

Stripe and QuickBooks are both PCI DSS compliant processors. Card details are tokenized and encrypted on their side and never touch our servers. Payouts go straight to your own bank account.

Encrypted at rest and in transit

AES-256 at rest, TLS in transit. The keys to your connected accounts sit in a separate encrypted secrets store.

Independently assessed

Google CASA AL1, validated by TAC Security.

You trust Aventide with real information about your business, your clients and your money. We protect it at every layer: an independently assessed app, encrypted data, firm walls between businesses, and an AI whose drafts for clients wait for your approval.

The short version

- **Independently assessed.** Google CASA at Assurance Level 1, validated by TAC Security in September 2026.
- **Encrypted in transit and at rest.** The keys to your connected accounts sit in an encrypted secrets store.
- **Walled off.** Our server checks which business you belong to on every request. Browsers can't change our database directly.
- **No passwords or card numbers stored by us.**
- **AI that asks first.** Aventide's AI uses your sign-in, stays inside your business, and asks before it sends, publishes, shares, cancels, voids or deletes anything.
- **Locked vault items stay out of Aventide's AI,** except a Smart Compliance scan you choose.
- **Every code change is checked.** No app code ships until it passes automated security, test and build checks.
- **In the United States, on audited infrastructure.** Our app servers and database run in the United States, on providers with independent SOC 2 Type 2 audits.
- **Found a security issue?** Email support@aventide.ai. Good-faith research is welcome; the rules are on aventide.ai/security.

For your security review

If a client or their IT team is checking Aventide, this is what we can show today. We hold one independent assessment of our app, we run on audited infrastructure, and we publish the documents a review asks for. We will never claim a certification we don't hold, and we answer security questionnaires by email.

- **Independent assessment:** Google CASA, Assurance Level 1, validated by TAC Security in September 2026.
- **Infrastructure audits:** Vercel, Supabase, Anthropic and Cloudflare each publish an independent SOC 2 Type 2 report; Stripe is certified PCI DSS Level 1 and QuickBooks Payments is a PCI DSS compliant processor, both on the owner's own account; card details are tokenized on their side and payouts go straight to the owner's bank.
- **Sub-processors:** the full list of companies that handle your data, with what each one does, on our [sub-processor page](#).
- **Data Processing Addendum:** our [DPA](#) for customers who need one, including the transfer terms our providers sign.
- **Where data lives:** the United States (Vercel, Supabase on AWS), backed up daily and kept 7 days.
- **Your data, out:** the account owner can have a ZIP of the account's data emailed from Your data, in the profile menu, or ask us for a full copy by email.
- **Your data, gone:** deletion on request by email, confirmed in writing.
- **If something goes wrong:** we tell you by email without undue delay; for your clients' data, we aim for 24 hours and never more than 72.
- **E-signatures:** consent and disclosure before signing, a frozen copy, an append-only record with the signer's IP and time, and a SHA-256 fingerprint on every signed document, as the US ESIGN Act and UETA require.
- **Your sign-in:** sign in with Google, which carries your Google 2-step verification, or with an emailed link; passwords are checked and stored by Outseta, never by us.
- **Questionnaires:** send us yours (SIG Lite, CAIQ, your own) and we answer it. support@aventide.ai

We're a US company and our customers are in the United States first. For anyone who needs it, we provide the pieces the GDPR and the CCPA ask of a provider: a Data Processing Addendum, a public sub-processor list, a copy of your data on request, deletion on request, breach notice within 72 hours, and no sale of personal data, ever.

Your money stays yours

Your clients' payments go into your own Stripe account: the one you already have, connected through the Aventide Stripe App, or one we set up for you on Stripe. Aventide doesn't hold the money and takes no cut. Refunds and disputes are handled in Stripe.

AI that stays in its lane

It uses your sign-in. When Aventide’s AI does something for you, it passes the same server checks you do, so it can only reach the business you’re working in.

It asks first. Aventide drafts freely, then asks for your approval before it sends an email or invoice, publishes or schedules a post, shares a document, books or cancels a meeting, voids a contract or invoice, or deletes a client, document, invoice or business. A contract goes to a client only after someone on your team countersigns it in the app.

Your data doesn’t train AI models. Our AI runs on Anthropic’s Claude models, usually reached through Vercel’s AI Gateway, which may also use the same models hosted by Amazon Bedrock or Google Vertex AI. None of them trains its models on data sent through their commercial services, and we don’t train AI models on your data either.

Built on audited infrastructure

Provider	What it does for us
Vercel	Hosts the app and routes AI requests (AI Gateway)
Supabase	Database, some file storage, live updates
Cloudflare	Most file storage and delivery, bot checks
Anthropic	AI models (Claude)
Amazon Web Services / Google Cloud	Backup hosts for the same AI models (through Vercel’s AI Gateway)
Outseta	Login and subscription billing
Stripe	Payments, for our billing and for your clients’ payments
Resend	Email we send to you and on your behalf

Vercel, Supabase, Anthropic and Cloudflare each publish independent SOC 2 Type 2 reports, and Stripe is certified PCI DSS Level 1. Those audits cover their own systems; our CASA assessment covers Aventide’s own app. The full list of providers that handle personal data is on our [sub-processor page](#).

What we don’t have yet

Our own SOC 2 report. Our core providers have theirs, and CASA covers our app. We’ll never claim a certification we don’t hold.

The full page, with how data is encrypted, where it lives, how businesses are walled off, safe links for clients, records you can rely on, deleting your data and how code ships, is at [aventide.ai/security](#).

Source: [aventide.ai/security](#), last updated October 17, 2026.