Collection Pilot

A product of The Well-Designed Firm

Security & Trust FAQ

Plain-English answers to questions every art-advisory firm should ask

Issued: May 27, 2026

For the longer, IT-grade version, see our Trust & Security Overview or write to security@collectionpilot.com.

The basics

Who actually owns my data?

You do. Our Terms of Service state this in writing: Customer Data remains the property of the Customer. We hold a limited license to it solely so we can operate the service for you. We never sell it. We never share it with marketers. We never use it to train AI models.

Can I export my data?

Yes — anytime, in standard formats. Every primary view in Collection Pilot (Acquisitions, Artists, Galleries, Collections, Contacts, Documents) has a one-click CSV export. For a full structured export of your entire workspace, email us and we'll deliver it within two business days at no charge.

Where is my data stored?

On Supabase's database and storage infrastructure, which runs on Amazon Web Services in the US East (Ohio) region. Encrypted at rest with AES-256. We do not maintain a separate AWS account — Supabase operates the underlying cloud for us. EU data residency is available on our Enterprise plan if you need it.

Do you use my data to train AI?

No. Not for our own AI, not for any third party's. The optional AI features inside Collection Pilot (like document summarization) call Anthropic's Claude API, which contractually does not train on the data sent to it. Your data stays yours.

Security

Is Collection Pilot SOC 2 certified?

Collection Pilot is built on infrastructure that is SOC 2 Type II certified: Supabase for our database and storage, Vercel for hosting, AWS for the underlying cloud. Application-layer SOC 2 Type II for Collection Pilot itself is on our roadmap as the customer base grows. We are happy to walk through our current posture in detail with your IT team.

How is my data encrypted?

In transit: TLS 1.2 or higher on every connection (your browser to our servers). At rest: AES-256 on the database, on file storage, and on all backups. Standard enterprise-grade encryption.

Who at Collection Pilot can see my data?

A small number of authorized employees of The Well-Designed Firm have administrative access for the purpose of operating the service. That access is logged, requires multi-factor authentication, and is never used to read your business data except (a) in response to your support request or (b) to diagnose a service-affecting incident. We have no offshore contractors and no third-party support firms.

Can other customers see my data?

No. Every database query is protected by **Row-Level Security** — a Postgres-enforced policy that makes it physically impossible for one customer's data to be returned in response to another customer's query, even if the application had a bug.

Do you support two-factor authentication?

For organizations that sign in with Google OAuth, two-factor authentication is enforced by your Google Workspace admin and applies before Collection Pilot ever sees the login — so anything your IT requires (TOTP, security key, hardware token) flows through automatically. A first-party MFA enrollment flow for email/password accounts is on our roadmap.

Do you support Single Sign-On?

SAML 2.0 SSO is available on the Enterprise plan. Email us if your organization needs it.

Reliability

What's your uptime?

We operate to a 99.9% monthly target — about 44 minutes of unplanned downtime per month at the floor. In practice we run higher than that. Our underlying providers (Vercel, Supabase) publish their own status pages and historically run above 99.9% as well.

How often is my data backed up?

Daily, included with every plan. Supabase performs automated daily backups of the Postgres database, with the last 7 days of snapshots available for restore at any time. Your uploaded files (PDFs, images, contracts) are replicated across multiple AWS availability zones for durability.

If your firm requires tighter recovery — for example, the ability to restore to a specific minute or even second within the last week — we can enable **Continuous Point-in-Time Recovery (PITR)** for an additional fee. The cost depends on the retention window you choose (7, 14, or 28 days). Ask during contracting and we'll quote it for you.

What if there's an outage?

You'll see it on our status feed inside the app. For confirmed security incidents that affect Customer Data, we commit in writing to notify you within 72 hours (the GDPR standard) by email to your account's billing contact.

What if you go out of business?

This is the most important question, and the most overlooked. Here is how we answer it.

How do I know I can get my data back if something happens to you?

Three layers of protection:

1. **The product gives you the data.** CSV export is built into every view; full workspace export is one email away. You can — and should — schedule recurring exports to your own storage today.
2. **The contract guarantees the right.** Your right to export Customer Data at any time during the Term and for 30 days after termination is contractually guaranteed and survives our bankruptcy, acquisition, or change of control.
3. **Wind-down notice.** Our Terms commit us to at least 90 days' written notice before discontinuing the service, during which you retain full access.

Is there source code escrow?

For Enterprise customers, yes — we'll arrange a code escrow agreement with a recognized third-party agent (Iron Mountain, NCC Group, or similar). The escrow agent holds the source code under sealed conditions and releases it to you under defined trigger events (vendor bankruptcy, discontinuation, material breach).

Who owns the company?

Collection Pilot is operated by **The Well-Designed Firm**, a New York-registered business owned and operated by founder Steven Burns under a business certificate (DBA), in continuous operation since 2022. The business is bootstrapped — no outside investors with liquidation preferences who could force a fire sale and change your terms. Founder and operational leadership has been continuous since the business was established. Happy to discuss the structure in more detail with serious prospects under NDA.

What about an acquisition?

The Assignment clause in our Terms requires our consent for material changes to your terms following any change of control. Data ownership, your export rights, and our deletion obligations survive an acquisition.

Privacy and compliance

Do you comply with GDPR?

Yes. Collection Pilot acts as a Processor for Customer Data and signs Data Processing Addenda incorporating the Standard Contractual Clauses for cross-border transfers. Email us to request a DPA.

What about CCPA?

We do not sell or share personal information as defined by California's CCPA / CPRA. Our Privacy Policy describes what we collect and the rights of California residents.

What about HIPAA?

Collection Pilot is not currently positioned for HIPAA-regulated workloads. If you have a specific use case involving Protected Health Information, please raise it during evaluation.

The discipline we recommend regardless

Even with all of the above, sound continuity discipline means not putting all your eggs in any one vendor's basket. We recommend every customer:

1. **Schedule a recurring export** — monthly is fine — to your own cloud storage (Dropbox, Google Drive, S3, your office NAS). Test that the export opens correctly in Excel.
2. **Document your processes outside Collection Pilot.** If the only place your firm's workflow is written down is inside our product, you're more locked in than you need to be.
3. **Run a parallel for the first 30 days.** Keep your current process running alongside Collection Pilot for the first month of paid use. It's a free, reversible test of whether the product fits.

We will help you do all three of these.

Send us your questionnaire

If your IT team or counsel has a security questionnaire — SIG, SIG-Lite, CAIQ, or a custom form — send it to **security@collectionpilot.com** and we will return a written response within 5 business days.

Serious vendors expect this. We do.