

Confidentiality & Data Handling Statement

How PhotoCAD handles customer images — and what PhotoCAD Stealth adds for confidential material.

PhotoCAD Stealth pins your conversions to AI providers under contractual no-training terms, locks out administrative access by default — any deliberate access is logged — and automatically destroys your files on a schedule you control. An NDA is included as part of Stealth agreements.

NO AI TRAINING

PhotoCAD never trains AI models on your images or your results, on any plan. On PhotoCAD Stealth, processing is additionally pinned to providers whose commercial terms prohibit using customer content, inputs or outputs, to train or improve their models — a contractual commitment, not a marketing statement. We do not name our AI providers publicly; for enterprise agreements, we disclose the full list with their data terms under NDA.

RETENTION & DELETION

	Standard accounts	Stealth accounts
While you keep a conversion	Stored until you delete it	Auto-deleted after 30 days by default (configurable); individual drawings can be pinned to keep
When you delete a conversion	Content permanently destroyed within 30 days	Content permanently destroyed within 48 hours

“Permanently destroyed” means image files and vector geometry are deleted from live systems and are not recoverable. Image files are never included in database backups, so no backup copy lingers. What remains is the billing record only — title, dates, credit charges, processing timings — nothing that contains or can reconstruct an image. Database records may persist in encrypted backups for up to 7 days before those backups expire.

ACCESS

- **No other user** can access your content: enforced at the database layer (row-level security) and storage layer (signed, expiring URLs).
- **Machines, not people:** images are processed entirely by automated systems; nobody at PhotoCAD reviews them in normal operation.
- **Stealth accounts** are excluded from all administrative views. Any deliberate access requires an explicit break-glass step, logged with a timestamp.

SECURITY & INFRASTRUCTURE

- TLS 1.2+ in transit, AES-256 at rest; storage URLs signed with 1-hour expiry.
- Data hosted on Supabase infrastructure in the United States (AWS us-east-2). AI processing runs on US-based providers; international transfers are covered by provider DPAs and standard contractual clauses.
- Infrastructure independently certified: Supabase (SOC 2 Type II, on AWS), Vercel (SOC 2 Type II), Stripe (PCI DSS Level 1). Card data never touches PhotoCAD servers.
- Passwordless sign-in by single-use, expiring magic link — no stored passwords.
- Vulnerability reports: security@photocad.ai — triaged on receipt, fixes prioritized over feature work.

SUB-PROCESSORS

Provider	Role	Data terms
AI providers	Image conversion (disclosed under NDA)	Independently certified (SOC 2 / ISO 27001). Stealth processing is pinned to the provider chain with contractual no-training terms and a DPA in place
Supabase	Database, storage, authentication	DPA; SOC 2 Type II
Vercel	Hosting and compute	DPA; SOC 2 Type II
Resend	Transactional email (never sees your images)	SOC 2 Type II
Stripe	Payments (never sees image content)	DPA; PCI DSS Level 1

WHAT WE DO NOT CLAIM

We are a small company and do not hold SOC 2 or ISO 27001 certification ourselves — our infrastructure providers do, and certification is on our roadmap as the business grows. We do not claim “zero retention”: the billing records and bounded backup windows above are the honest shape of it, and none of it contains your images. We complete security questionnaires and vendor review forms for business customers.

CHANGES

Material changes to anything in this statement — how or where content is processed, longer retention, weaker guarantees — carry at least 30 days’ notice by email to affected accounts.

This statement reflects PhotoCAD's systems as of the version date above and corresponds to photocad.ai/trust. It describes data handling practices and is not legal advice. Questions: support@photocad.ai.