TRUST DOCUMENT

Data & Security Overview

How your data is stored, protected, and backed up

Stone Creek Surfaces / StoneIQ | Knoxville, Tennessee | Effective June 13, 2026
stoneiqmicro.app

> AI-assisted development has made it faster than ever to build and ship software — and that is a genuinely good thing for every industry, including ours. But speed without structure creates risk. Not every tool marketed for professional or enterprise use has been architected to the standard that title implies. We built StoneIQ Micro with security and data integrity as first-class concerns from day one. This document exists so you can verify that for yourself.

StoneIQ Micro is built for small stone shops, and we take seriously the fact that you're trusting us with your customer info, job records, and business data. This page explains exactly how your data is stored, who can access it, and what protections are in place. No buzzwords — just a straightforward account of how the app is built.

Where your data lives

Your data is stored in a PostgreSQL database hosted by Supabase on Amazon Web Services, in the us-east-1 (Northern Virginia) region. The app itself runs on Vercel's global edge network, which handles HTTPS termination and serves the application from data centers close to your location. File uploads (slab photos, logos) are stored in Supabase Storage, which is backed by AWS S3 in the same region.

How your data is isolated

Every shop on StoneIQ Micro has its own isolated slice of the database. This isolation isn't just a setting in the app code — it's enforced directly at the database layer using PostgreSQL Row-Level Security (RLS).

Here's what that means in plain terms: every query that touches the database automatically includes a rule that says "only return rows that belong to this shop." It's not possible for one shop's session to read or modify another shop's quotes, jobs, contacts, or any other records — the database itself rejects those queries before they're even processed. Even if there were a bug in the application layer, the database-level policy would still block cross-shop data access.

How we protect your account

Authentication is handled by Supabase Auth. Sessions are managed with secure, HTTP-only cookies — your session token is never exposed to JavaScript running in the browser, which protects against a common class of attacks.

When you set a password, StoneIQ checks it against a database of known compromised passwords (via Supabase's leaked-password protection). If your chosen password has appeared in a known data breach, you'll be asked to pick a different one. This runs at sign-up and password change — before anything is saved.

Payment security

StoneIQ uses Stripe for all payments. Your card number, CVC, and billing details are entered directly into Stripe's secure hosted fields and never touch StoneIQ's servers. We store only what Stripe gives back: a customer ID and subscription status.

Stripe is a PCI DSS Level 1 certified payment processor — the highest level of payment industry compliance. We never see or store raw card data.

One deliberate design choice: no writes are allowed to your account until payment is confirmed. This is enforced in both the API middleware and the database policies — not just the UI. It means no one can create trial accounts to probe the system or generate junk data.

File & photo storage

Files are split into two buckets in Supabase Storage (AWS S3-backed):

- Public bucket — shop logos, which are intentionally public for display purposes.
- Private bucket — slab photos and other job-related files. These are never directly accessible via a public URL.

All file uploads and downloads for the private bucket go through signed URLs generated on the server. Your browser never talks directly to S3 with credentials — it requests a short-lived, single-use URL from our API, which the server only issues after verifying you have access to that file. Signed URLs expire quickly and can't be reused.

Email communications

Transactional emails (receipts, notifications, account messages) are sent through Resend. The stoneiqmicro.app domain has SPF, DKIM, and DMARC DNS records configured. This means:

- Email clients can verify that messages from stoneiqmicro.app actually came from our authorized sending infrastructure.

- Spoofed emails claiming to be from StoneIQ are more likely to be caught and rejected by mail servers.

We don't send marketing email. You'll only hear from us when something happens on your account.

Backups & uptime

Supabase runs automated daily backups of the database. On the Pro plan, point-in-time recovery is available, meaning we can restore to any point within the retention window — not just to the last nightly snapshot.

Deployments on Vercel are zero-downtime — new versions are deployed atomically and traffic is only shifted once the new build is healthy. There's no maintenance window that takes the app offline.

Security headers & transport

All traffic to StoneIQ Micro is served over HTTPS. The following HTTP security headers are set on every response:

Header	Value
Strict-Transport-Security	2-year max-age, forces HTTPS for all future visits
X-Frame-Options	DENY — prevents the app from being embedded in iframes (clickjacking protection)
X-Content-Type-Options	nosniff — prevents browsers from guessing file types
Referrer-Policy	Strict — limits what URL info is sent to third parties
Permissions-Policy	Camera, microphone, and geolocation all disabled

HSTS with a 2-year duration means your browser remembers to always use HTTPS for stoneiqmicro.app — even if you type the address without https://.

Dependency monitoring

We use GitHub Dependabot to automatically scan for known vulnerabilities in npm packages on a weekly basis, and GitHub Actions dependencies on a monthly basis. Security patches are reviewed and merged promptly. We also use Sentry for real-time error monitoring on both the server and client — unusual errors surface immediately rather than going unnoticed.

Your data rights

You own your data. Full stop.

- Export: From your account settings, you can export all your quotes, jobs, and contacts as CSV or PDF at any time. No need to contact us.
- Deletion: You can delete your account from settings. This permanently removes your shop's data — customers, jobs, quotes, files, and all associated records. Deletion is irreversible, and we'll confirm before proceeding.

We don't sell your data, share it with advertisers, or use it to train anything.

Reporting a security issue

If you find a vulnerability or something that looks wrong, please email us directly at support@stoneiqmicro.app. We'll respond promptly and treat the report seriously. Responsible disclosure is appreciated — give us a reasonable window to investigate before going public, and we'll do the same for you.