SECURITY BRIEF

StashGrade

How we protect your financial data. A companion to stashgrade.com/security.

Read-only access

We only **read** your accounting data (QuickBooks and any source you connect). StashGrade cannot create, edit, or delete anything in your books, and it cannot move money.

Encryption everywhere

TLS in transit with HSTS; data encrypted at rest. Connection tokens are additionally encrypted with AES-256-GCM before storage and never written to logs.

Payments stay with Stripe

Billing runs through Stripe (PCI DSS Level 1). Your card details go directly to Stripe. StashGrade never receives or stores your card number.

Benchmarks: opt-in, anonymized

Off by default. If you opt in, your figures join the pool under a one-way identifier, in cohorts of five or more, never with your name, customers, or transactions. Opt out and your data leaves.

Isolated at the database

Every company's data is locked with forced row-level security enforced by the database itself, not just app code. An automated cross-company test proves the isolation on every deploy.

Application security

Every request is authenticated and ownership-checked. Webhooks are signature-verified, third-party connections are CSRF-protected, no secrets reach the browser, and secret, dependency, and static scans run on every change.

AI data handling

Analysis runs on Anthropic's Claude API, where your data is not used to train models and is never shared with public models. Every call is bounded by hard, fail-closed spend caps.

Hosting, retention, deletion

Hosted in the United States on Vercel and Supabase (SOC 2 Type II). We never store your card or QuickBooks password. Disconnect or request deletion anytime; data export on request.

Sub-processors

Intuit / QuickBooks (you authorize the connection) • Supabase, database, SOC 2 Type II • Vercel, hosting, SOC 2 Type II • Stripe, payments, PCI DSS Level 1 • Anthropic, AI analysis, SOC 2 Type II • Resend, email, SOC 2. Certifications as published by each provider.

Compliance posture, honestly

StashGrade is built on SOC 2 Type II infrastructure and follows secure-by-default engineering: least privilege, encryption, database-enforced isolation, and automated security testing on every release. In progress: our own SOC 2 Type II examination (available under NDA), an independent third-party penetration test, and optional multi-factor authentication. We do not claim certifications we do not hold.

Operated by However We Got Here, LLC. Security questions or good-faith vulnerability reports: info@howeverwegothere.com. Full detail and our access model: stashgrade.com/security.