Security Notice

How we protect the information you trust us with, particularly the investigation files, which are among the most sensitive records there are.

Effective May 20, 2026 · Next scheduled review November 20, 2026

We maintain administrative, technical, and physical safeguards designed to protect information from unauthorized access, alteration, disclosure, or destruction. Our controls are proportional to the sensitivity of the data, and the data we handle in investigations is as sensitive as it gets.

Access control

Access to client and engagement data is restricted to authorized personnel with a need to know, granted on a least-privilege basis and reviewed regularly. Access to active investigation files is logged and audited.

Encryption

Data is encrypted in transit using TLS and at rest. Credentials are stored using industry-standard hashing. We never store full payment card numbers, which are handled by Stripe.

Where data lives

Application data and authentication run on Supabase, in United States data centers; Supabase is SOC 2 Type II compliant. Active investigation files and privileged work product are held separately on firm-managed private infrastructure in United States data centers, storage we control directly, because the sensitivity of that material requires it.

Subprocessors

We use a small, vetted set of subprocessors, each bound by a written data processing agreement and each SOC 2 Type II audited where applicable. The current list, with the data each one handles, is in our Privacy Policy.

Segregation of sensitive records

Investigation files are segregated from general application data. They are never used to train artificial intelligence systems, and they are never anonymized and republished without the engaging institution’s written consent.

Breach notification

No system is perfectly secure. If we become aware of a breach affecting personal information, we notify affected individuals and applicable regulators in accordance with applicable law, without undue delay.

Responsible disclosure

If you believe you have found a security vulnerability affecting Fractional Coordinator, write to security@fractionalcoordinator.com. We appreciate responsible disclosure and will acknowledge your report.

Changes to this notice

We update this notice as our practices evolve. The effective date above reflects the most recent change.