SECURITY & COMPLIANCE

# Built for the standards you already enforce.

A technical overview of InFocus Pathways' security architecture, data controls, and regulatory compliance posture — written for IT teams, security officers, and technology leaders at nonprofit, workforce, and school partners.

DOCUMENT DATE
May 22, 2026

COMPLIANCE FRAMEWORKS
FERPA · COPPA · SOC 2 (in progress)

CONTACT
info@infocuspathways.com

# Regulatory Compliance

InFocus operates at the intersection of participant privacy and career development. Every architectural decision maps back to one of the frameworks below. FERPA, COPPA, and the "school official" designation described here apply specifically to our school-partner deployments — the same underlying commitments (customer data ownership, minimal necessary access, full audit logging) are the baseline for every InFocus customer, including nonprofit and reentry-program partners not subject to those specific statutes.

## FERPA

**Family Educational Rights and Privacy Act**

InFocus acts as a "school official" under FERPA — accessing student education records only to perform contracted services. The school retains ownership and control of all records at all times. No student data is disclosed to third parties without explicit written authorization from the school, except as required by law.

## COPPA

**Children's Online Privacy Protection Act**

InFocus does not permit direct student account creation. All student records are created and managed by authorized school personnel. Schools attest in the signed DPA that they hold parental consent authority under COPPA. No advertising, behavioral tracking, or third-party analytics are present on any student-facing surface.

## SOC 2

**Service Organization Control Type II**

InFocus is architected to meet SOC 2 Type II Trust Service Criteria (Security, Availability, Confidentiality). Formal audit engagement is in progress. Controls are implemented across access management, encryption, monitoring, change management, and incident response.

## DATA PROCESSING AGREEMENT

**DPA required before any student data is entered**

Every school must execute a signed Data Processing Agreement (DPA) before student records can be created in the platform. The DPA establishes InFocus as a data processor, defines data ownership (the school), enumerates all subprocessors, and includes the COPPA attestation. No student PII is collected without an active, signed DPA on file.

## WHAT WE COMMIT NOT TO DO

- **No sale of participant data.** Participant data is never sold, licensed, or transferred to any third party for commercial purposes.
- **No advertising or behavioral targeting.** No advertising pixels, tracking scripts, or behavioral profiling on any page of the platform — including marketing pages.
- **No cross-organization data access.** Row-level security at the database layer enforces strict organization-level data isolation. No query can return records belonging to a different organization.
- **No third-party analytics on participant surfaces.** Tools like Google Analytics, Segment, or Mixpanel are absent from all authenticated routes.

# Where Your Data Lives

InFocus is built on a small, auditable set of subprocessors — each with a signed DPA. No subprocessor that touches participant PII may be added without notifying existing customers and updating the DPA.

| Vendor | Role | Participant PII | Data Region |
|---|---|---|---|
| **Supabase** | Primary database & file storage | **Yes — full records** | US (AWS us-east-1) |
| **Railway** | Next.js application hosting | In transit only | US |
| **Cloudflare** | TLS termination, DNS, DDoS protection, CDN | In transit only | Global edge |
| **Resend** | Transactional email delivery | Report delivery only | US |
| **Stripe** | Subscription billing | No | US |
| **Upstash Redis** | API rate limiting | No | US |

## DATABASE SECURITY

- **Row-level security (RLS)** Enforced at the Postgres layer via Supabase RLS policies. Application-level bugs cannot expose cross-school data — the database rejects the query.
- **No public storage buckets.** All file storage (PDF reports, attachments) uses private Supabase Storage buckets. Files are accessed only via signed URLs with a 15-minute expiry.
- **Encryption at rest.** All data is encrypted at rest by Supabase (AES-256). Encryption is managed at the storage layer.
- **Encryption in transit.** TLS 1.2+ enforced for all connections. HTTPS Strict Transport Security (HSTS) header with a one-year max-age is set on all responses.

## DATA ISOLATION MODEL

**Multi-tenant, organization-scoped architecture**

Every record in the database carries an organization-scoping foreign key (schoolId in the schema — a legacy name from the platform's origin that now scopes any customer organization, including nonprofits and reentry programs). All API routes validate the authenticated user's organization against the requested resource before any read or write operation. This check is enforced at both the application layer and the Supabase RLS layer — two independent enforcement points for the same isolation guarantee.

## SCORING ARCHITECTURE

- **Server-side only.** All assessment scoring — career interest clusters, RIASEC coding, RML ratings, aptitude derivation, and program comparison — is performed server-side in Node.js. No scoring logic executes in the client browser.
- **No raw answer transmission to third parties.** Participant assessment responses are stored in the InFocus database and never forwarded to external AI services, analytics platforms, or data brokers.

# Identity & Access Management

InFocus enforces layered access controls across authentication, session management, and role-based permissions. Controls are not optional — they are architectural.

## AUTHENTICATION

- **Multi-factor authentication (MFA) — mandatory.** All Program Administrator and Case Manager accounts must complete TOTP-based MFA enrollment before accessing any participant data. MFA cannot be bypassed or disabled by end users.
- **Password hashing.** Passwords are hashed using bcrypt with a cost factor of 12. Plaintext passwords are never stored, logged, or transmitted.
- **Account lockout.** Accounts are locked after 5 consecutive failed login attempts. Lockout requires administrator intervention to release.
- **90-day password expiry.** Admin and Case Manager roles are required to reset passwords every 90 days. The platform enforces this at login — expired credentials cannot proceed.
- **Session management.** Authenticated sessions use signed, HttpOnly cookies with an 8-hour lifetime. Sessions are invalidated on logout and on password change.

## ROLE-BASED ACCESS CONTROL

| Role | Permissions | MFA Required |
|---|---|---|
| **Program Admin** | Full platform access — manage users, billing, data rights, DPA, all participant records within their organization | Yes |
| **Case Manager / Evaluator** | Create and manage participant records, administer assessments, enter InFocus Aptitude scores, generate reports | Yes |
| **Participant (read-only)** | View own assessment results and reports only — no access to other participants or administrative functions | No |

For school-partner deployments, these roles map to the FERPA-context terms School Admin, Counselor, and Student used elsewhere in this document.

## SESSION & COOKIE SECURITY

- **HttpOnly cookies.** Session tokens are stored in HttpOnly cookies — inaccessible to JavaScript, mitigating XSS-based session theft.
- **SameSite=Lax.** Cookies carry the SameSite=Lax attribute, protecting against CSRF attacks on state-mutating requests.
- **Secure flag.** Cookies are marked Secure — transmitted only over HTTPS connections.
- **MFA-verified cookie.** A separate mfa_verified cookie tracks MFA completion within a session. Routes requiring MFA verify both the session and MFA cookies independently.

# Network & Application Security

Transport-level protections, HTTP security headers, and rate limiting form the perimeter of the InFocus application layer.

## TRANSPORT SECURITY

- **HTTPS enforced globally.** All HTTP traffic is permanently redirected to HTTPS. Plain HTTP connections are rejected at the edge.
- **HSTS.** HTTP Strict Transport Security header with max-age=31536000 (one year) instructs browsers to refuse non-HTTPS connections, even on first visit.
- **TLS 1.2+ only.** Legacy TLS 1.0 and 1.1 are not supported. Cipher suites are managed by Cloudflare's edge infrastructure.

## HTTP SECURITY HEADERS

- **Content Security Policy (CSP).** A nonce-based CSP is generated per request and injected into all HTML responses. Inline scripts require the correct nonce — no bare unsafe-inline for script-src.
- **X-Frame-Options: DENY.** Prevents the application from being embedded in iframes — mitigating clickjacking attacks.
- **X-Content-Type-Options: nosniff.** Prevents browsers from MIME-sniffing responses away from the declared content type.
- **Referrer-Policy: strict-origin-when-cross-origin.** Limits referrer information sent to third-party origins.

## RATE LIMITING

- **API rate limiting via Railway Redis.** All authentication endpoints (login, MFA verify, password reset) are rate-limited. Burst limits prevent credential stuffing and brute-force attacks.

## AUDIT LOG

> **Append-only audit log — 28+ tracked event types**
> Every significant action in the platform writes an immutable audit log entry. Logs are append-only — no record can be modified or deleted. Minimum retention is 7 years. The audit log is accessible to Program Administrators from the dashboard and is available for export upon request.

| Event Category | Examples |
|---|---|
| **Authentication** | Login, logout, failed login, MFA enrollment, password change, account lockout |
| **Participant records** | Record created, updated, soft-deleted, restored |
| **Assessment activity** | Assessment started, completed, InFocus Aptitude scores entered, reset |
| **Reports** | Report generated, report shared, report viewed |
| **Data rights** | Export requested, deletion requested, DPA signed |
| **Administration** | User invited, role changed, case manager assigned, billing updated |

# Data Rights & Retention

Organizations retain full ownership and control of their data throughout the subscription lifecycle and beyond.

## RETENTION POLICY

- **Participant records.** Retained for a minimum of 7 years from the date of last activity, consistent with FERPA records guidance for school partners. Organizations may request a shorter retention window.
- **Audit logs.** Append-only, retained for a minimum of 7 years. Cannot be shortened.
- **Post-cancellation.** Upon subscription cancellation, organization data remains available for export for 90 days. After 90 days, all data is permanently deleted. A deletion confirmation is provided.
- **No hard deletes during subscription.** All deletion requests during an active subscription are fulfilled via soft-delete — the record is hidden from the UI but retained with a full audit trail. This satisfies FERPA's requirement for records of disclosure for school partners.

## DATA RIGHTS

- **Full data export.** Program Administrators can request a full JSON export of all participant data from the Data Rights panel in Settings. Exports are logged to the audit trail.
- **Individual participant deletion.** Organizations may submit a deletion request for any individual participant record. Requests are reviewed and fulfilled within 30 days.
- **DPA termination rights.** Either party may terminate the DPA with 30 days written notice. InFocus will provide a data export and confirm deletion within the contractual window.

## INCIDENT RESPONSE

> **72-hour breach notification commitment**
>
> In the event of a confirmed data breach affecting participant PII, InFocus will notify affected organizations within 72 hours of discovery — consistent with FERPA breach notification guidance for school partners and common state data breach laws. Notification will include: nature of the incident, data categories affected, remediation steps taken, and a point of contact for the organization's IT team.

- **Written Incident Response Plan (IRP).** InFocus maintains a documented IRP covering detection, containment, eradication, recovery, and post-incident review.
- **Vulnerability disclosure.** Security researchers and IT contacts may report suspected vulnerabilities to info@infocuspathways.com. We commit to acknowledging reports within 2 business days.
- **Vendor security monitoring.** Supabase, Railway, and Cloudflare security advisories are monitored continuously. Critical patches are applied within 24 hours of release.

## CONTACT FOR SECURITY REVIEW

### Security & Compliance Inquiries

For vendor security questionnaires, DPA review, penetration test scheduling, or compliance documentation requests, contact:

### Additional Documents Available

- Data Processing Agreement (DPA)
- Subprocessor list with DPA status

**info@infocuspathways.com**

- Privacy Policy (infocuspathways.com/privacy)
- Terms of Service (infocuspathways.com/terms)
- SOC 2 report (available upon NDA execution)

**"Potential is universal. Opportunity is not."**

InFocus Pathways exists to give every participant — regardless of background or starting point — a clear, evidence-based path forward. The security controls in this document exist to protect that mission and the people it serves.