Security Overview

APEX Coach AI
Last Updated: March 2026

Infrastructure

- Supabase for authentication, database services, and server-side data operations
- Vercel for web hosting and deployment runtime
- Limited third-party providers for AI processing and account-related email delivery

Authentication

- User authentication is managed through Supabase Auth.
- Application routes and APIs enforce authenticated access for protected resources.
- Session handling is integrated with app middleware and role-aware access checks.

Access Control and Tenancy

- Access is scoped by role and organizational context (school, team, coach, athlete).
- Platform data access follows role-based access patterns and tenancy separation.
- Administrative write paths are restricted to controlled server-side service-role operations.

Encryption and Transport

Data in transit is protected over HTTPS/TLS endpoints. Password processing is handled by the authentication provider and not stored in plaintext by APEX application logic.

Logging and Auditability

APEX stores operational records that support reliability and audit workflows, including:

- Legal acceptance records
- Feature/usage event logs
- AI operation metadata and error context

These records are used to support service integrity and troubleshooting.

Incident Handling

APEX maintains internal incident documentation practices and operational runbooks for service disruptions. District-facing response expectations are governed by contract terms and supporting security documentation.

Vendor Management

Current subprocessors used in delivery of service include:

- Supabase
- Vercel
- OpenAI
- Anthropic
- Resend

Subprocessor updates are published on the APEX subprocessor page.

Scope Clarification

APEX is a coach workflow and accountability platform. It is not a medical system and does not provide medical advice, diagnosis, or treatment.