Security Overview

For district IT administrators, CISOs, and security reviewers.

Authentication Model

- Teachers: email + bcrypt-hashed password (10 rounds). Session-based auth with httpOnly cookies.
- Students: classroom join code (CYBER-XXXX format) — no passwords; no PII required to create an account.
- Principals: email + bcrypt-hashed password, scoped to their school only.
- Parents: email-only authentication via one-time claim token (single-use, expires after use).
- Admin panel: HTTP Basic Auth over HTTPS with environment-injected credentials.

Encryption

- In transit: TLS 1.2+ enforced on all endpoints. HTTP requests redirect to HTTPS automatically (301).
- At rest: Neon PostgreSQL database uses AES-256 encryption at the storage layer (AWS-managed KMS).
- Session secrets: stored as environment variables, never in source code or version control.
- OAuth tokens (if applicable): AES-256-GCM encrypted before database storage.

Data Residency

All student and teacher data is stored in the United States. Primary database: Neon PostgreSQL on AWS US-East. Application hosting: Render (US region). No student data is transferred to or stored in jurisdictions outside the United States.

Infrastructure & Network Security

- Application hosted on Render (SOC 2 Type II certified cloud platform).
- Database: Neon PostgreSQL — SOC 2 Type II, isolated per-project credentials, connection pooling via PgBouncer.
- No direct database access from student-facing code; all queries use parameterized statements (no raw string interpolation).
- Environment variables managed via platform secrets (not checked into version control).
- Dependency audit: npm audit run on each deployment; critical vulnerabilities block deploy.

Incident Response

CyberHeroesHQ maintains an internal incident response procedure. In the event of a confirmed breach involving Student Personal Information:

- Affected schools/districts notified within 72 hours of confirmed breach discovery.
- Notification includes: nature of data exposed, students affected (if known), steps taken to contain, and remediation timeline.
- Contact for security incidents: security@cyberheroeshq.com

Access Controls & Staffing

- Production database access requires MFA and is logged.
- Principle of least privilege: application credentials scoped to minimum required permissions.
- Student data is not accessible to support staff without a logged, purpose-limited request.

AI mentor (Cipher) receives only the current mission context and student answer — no personally identifiable information is sent to the AI provider.

Backups & Recovery

- Neon PostgreSQL: continuous WAL archiving + point-in-time recovery (PITR) up to 7 days.
- Recovery Time Objective (RTO): < 4 hours for full service restoration.
- Recovery Point Objective (RPO): < 5 minutes data loss window.

Vendor Questionnaires & Additional Review

For custom security reviews, HECVAT completion, or security questionnaire responses, contact security@cyberheroeshq.com. We aim to respond within 5 business days. For the full Trust & Compliance center including DPA download, visit:

https://cyberheroeshq.com/trust