



Technical Blueprint

Architecture, data handling, and network requirements for district IT evaluation

For district technology teams · Version 1.0 · policytoaction.beauhawked.com

1. Executive Summary

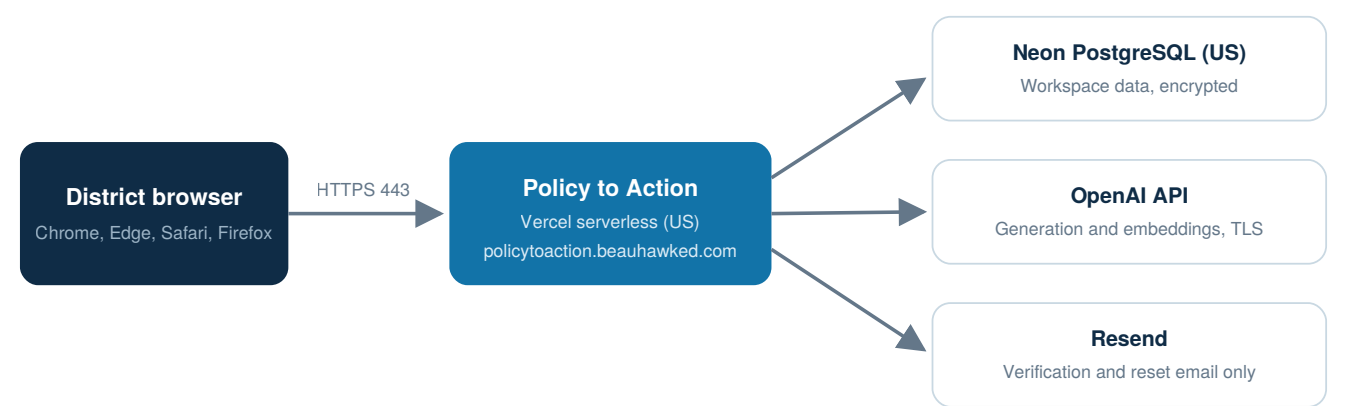
Policy to Action is a fully hosted, browser-based decision-support application for school district administrators. Users describe administrative scenarios in plain language and receive structured guidance generated exclusively from the district's own uploaded board policies and handbooks, with every claim cited to its source text.

From a district IT perspective, the essentials are: it is software as a service with nothing to install and no on-premises components; the client is a standard web application reached over HTTPS; no inbound connections to district networks are ever made; and the application is architected to operate without student personal information.

2. Technology Stack

Layer	Technology
Web application	Next.js 15 (React 19, TypeScript), server-rendered with a single-page client experience
Application hosting	Vercel serverless platform, United States region, TLS terminated at the edge
Database	Neon serverless PostgreSQL, United States region, encrypted at rest and in transit, with the pgvector extension for semantic retrieval
AI processing	OpenAI API (GPT-4.1 class generation model and text-embedding-3-small embeddings) over TLS
Transactional email	Resend, sending only account verification and password reset messages from the dedicated subdomain send.beauhawked.com

3. Architecture and Data Flow



The browser communicates only with policytoaction.beauhawked.com. All connections to the database, the AI provider, and the email service originate server side from the hosting platform, never from the user's device and never from inside the district network. The application initiates no inbound connections to district systems, requires no VPN, agent, or firewall exception beyond ordinary outbound web browsing, and integrates with no district directory or student information system.

What happens when a user asks a question

The scenario text travels over HTTPS to the application, which retrieves the most relevant passages from the district's own uploaded policies using combined lexical and semantic search, sends the scenario plus those passages to the OpenAI API for answer generation, stores the exchange in the district workspace, and returns

the cited answer to the browser. Every model interaction is additionally recorded in an append-only audit log capturing the full input, output, model identity, and timing.

4. Network Requirements

Requirement	Detail
Web access	Allow HTTPS (TCP 443) to policytoaction.beauhawked.com . All application assets, including fonts and icons, are served from this origin; no third-party domains are contacted by the browser.
Email delivery	Permit mail from no-reply@send.beauhawked.com (verification and password reset only). The sending domain publishes SPF, DKIM, and DMARC records.
Inbound connections	None. The application never connects into district networks.
Bandwidth	Negligible; text-based traffic comparable to ordinary web browsing.
Client requirements	Any current version of Chrome, Edge, Safari, or Firefox on desktop, Chromebook, tablet, or phone. No plugins, extensions, or local installation. Functions on managed devices with standard content filtering.

5. Authentication and Access Model

Accounts are individual, created with a verified work email address and password. Passwords are hashed with scrypt and never stored or transmitted in recoverable form. Sessions are managed server side with expiring identifiers in cookies; password reset and email verification use single-use, time-limited tokens stored only as SHA-256 hashes. Request rate limiting is enforced per account and address on authentication, questioning, and administrative endpoints. Each account's workspace, including its policies, conversations, and pinned answers, is isolated from every other account. Single sign-on integration is on the product roadmap and not yet available.

6. Data Handling

Data	Storage and handling
Board policies and handbooks	Uploaded by the district's designated administrator; these are typically public governance documents. Stored in the district workspace; district can archive or permanently delete at any time.
Scenario questions and answers	Stored per account as conversation history; deletable per conversation by the user. The interface coaches users on every screen to use placeholders such as Student A rather than real names.
Account data	Name, work email, district name, and password hash only. No directory synchronization and no student rosters.
Model audit log	Append-only record of AI interactions retained for accountability and reconstruction.
Student education records	Not collected, not required, and not part of the design. The platform operates on policy text, not student data.

All data is encrypted in transit (TLS) and at rest, and is hosted in United States regions. AI processing uses the OpenAI API under a Data Processing Addendum; API inputs and outputs are not used to train OpenAI models.

7. Application Security Controls

- Strict Content Security Policy in production: scripts, styles, images, fonts, and connections restricted to the application's own origin, with framing denied entirely.
- Hardened response headers: X-Content-Type-Options nosniff, X-Frame-Options DENY, strict referrer policy, camera, microphone, and geolocation disabled by Permissions-Policy, and cross-origin isolation headers.
- API responses are marked non-cacheable to keep workspace content out of shared caches.
- Server-side authorization on every data access; ownership of conversations, pins, and sources is verified against the session on each request.
- Dependency hygiene and security review as ongoing practice, with rate limiting as an abuse backstop.

8. Compliance Posture

Policy to Action is designed to operate without student personally identifiable information, which keeps districts' FERPA obligations with the systems that actually hold education records. The district remains the owner of its uploaded content. Users are adults (district staff), so child-directed service rules do not apply.

Answers are explicitly labeled as decision support rather than legal advice, and the citation model exists so administrators verify guidance against the governing source before acting. The in-application Trust and Privacy page (Help, then Trust and privacy) presents the data-handling statement and the full service-provider list for review, and the vendor welcomes district security questionnaires.

9. Operations

Item	Detail
Availability model	Serverless hosting with automatic scaling; no maintenance windows required for districts
Backups	Managed database platform with point-in-time recovery capability
Updates	Continuous deployment; districts receive improvements without action on their part
Data return and deletion	Districts can export policy datasets (Markdown) and delete sources and conversations directly in the product at any time
Support	Beau Scott, Scarlet Fire LLC, via your district's onboarding contact information

10. Summary for the Firewall Change Ticket

Minimum action for district IT: confirm HTTPS access to policytoaction.beauhawked.com from staff networks and permit email from no-reply@send.beauhawked.com. No other changes are required.

Policy to Action Technical Blueprint, Version 1.0. Statements reflect the current production architecture and are updated as the platform evolves. Guidance produced by the platform is generated from district-uploaded sources and is not legal advice.