Axiospec: Security and Data Handling

For IT and security reviewers. Axiospec is a calibration and asset record system built by CaliTech LLC, Knoxville, Tennessee. This page describes how the production service handles customer data. Everything below is a statement about production. Last reviewed: 19 August 2026.

Two things to know before you read further. Axiospec holds no security certifications today, and we say exactly what we do and do not have in the last section rather than making you dig for it. Axiospec is a record-keeping system. It supports and documents your calibration program and keeps it audit-ready. It does not certify, ensure, or guarantee your compliance with any standard.

Where your data lives

Amazon Web Services, single account, region **us-east-1 (Northern Virginia, United States)**. Every stateful production resource is declared in that one region: the PostgreSQL 16 database, the document storage bucket, the audit log bucket, secrets storage, and the application compute.

The content delivery network in front of the app (Amazon CloudFront) is a global edge network. It terminates TLS at an edge location that may be outside the US and forwards the request to us-east-1. API responses are explicitly configured **not** to be cached at the edge. Only static application and marketing assets are cached. Subprocessors listed below process data in their own locations.

Encryption

In transit. The application and API are served over HTTPS only. Plain HTTP is redirected. Minimum TLS version is 1.2. The connection from the CDN back to the application is also TLS 1.2. Database connections require TLS (`sslmode=require`), and the authentication service refuses to start against a database URL that does not require it.

At rest. The production database has storage encryption enabled. The infrastructure audit log bucket is encrypted with SSE-S3 (AES-256). Application secrets are held in AWS Secrets Manager and loaded at runtime rather than sitting in plaintext environment variables. The message queue used for failed background jobs uses SQS-managed encryption.

Uploaded evidence files (calibration certificates, photos) are stored in Amazon S3, which encrypts objects at rest by default with SSE-S3. We do not currently declare that setting explicitly in our infrastructure code, so we describe it as the platform default rather than as a control we evidence. All encryption uses AWS-managed keys. There is no customer-managed key (BYOK) option.

Network isolation

The production database is **not publicly accessible**. Its only inbound rule is PostgreSQL from the application's own security group. There are no IP ranges permitted. Deletion protection is on.

The application runs inside a VPC across two availability zones in private subnets with no public IP addresses. Outbound traffic goes through a NAT gateway; S3 traffic uses a VPC gateway endpoint and does not traverse the public internet. The application security group has no inbound rules at all.

All S3 buckets have public access fully blocked on all four settings. The single-page application bucket is readable only by our CloudFront distribution, enforced by Origin Access Control and a bucket policy scoped to that distribution. The application's write access to the document bucket is limited to `PutObject` and `GetObject` on that bucket only.

Tenant separation

Axiospec is multi-tenant: a shared database with a shared schema and **row-level tenant scoping enforced in the application**. Every customer-owned table carries a `tenant_id`. The tenant identity is read from a signature-verified token claim, never from a client-supplied header or request body. Core record types (instruments, ledger entries, users) are additionally filtered by a global query listener that injects the tenant condition on every read. Uploaded files are stored under tenant-prefixed object keys.

Be accurate about what this is: it is application-enforced isolation, not PostgreSQL row-level security, and not a separate database or schema per customer.

Inside a workspace, there is a second boundary. Site grants can restrict a user to specific plants or locations, and the server checks the site scope on record, approve, void, and export operations.

Authentication and access control

Passwords are hashed with PBKDF2-HMAC-SHA256 at 260,000 iterations with a per-password random salt, verified in constant time. Sign-in uses either an email and password or Google sign-in, which is live in production. Accounts created through Google have no usable password.

Brute-force protection is per-account exponential backoff, shared across all application instances at the database level, keyed on a hash of the identifier so a nonexistent account behaves identically to a real one. It is capped so it cannot be turned into a denial of service against your users.

Sessions use stateless signed tokens with a 7-day default lifetime, held in browser local storage. Deactivating or deleting a user takes effect immediately: account state is re-checked from the database on every request, so an existing token stops working on that user's next call. There is no generic revocation list, so a token stolen from a still-active user remains valid until it expires.

Role-based access control is enforced on the server, not in the browser. Five roles: super admin, admin, manager, technician, auditor. The role is re-read from the database on each request rather than trusted from the token. The auditor role is enforced as globally read-only, with a narrow allowance to generate an audit export. Managers cannot promote users above their own authority.

Two application controls that matter to a quality reviewer. Committed calibration records cannot be edited or deleted, enforced by a database trigger, so this holds even against direct SQL access. Corrections are appended as new linked records with a required written reason. And when a workspace turns on maker-checker review, the system refuses to let the person who recorded a calibration approve it.

Administrative console access controls for our AWS account are confirmed separately on request.

Backups and recovery

Automated daily database backups with a **14-day retention window**, which supports point-in-time recovery within that window. Deletion protection and a mandatory final snapshot are enabled. Infrastructure alarms are configured in CloudWatch for database CPU, storage, and connection pressure, application errors, throttling, latency, CDN 5xx rate, and failed background jobs, and are delivered to an on-call email address.

Honest limits: the production database is single availability zone. An AZ failure requires a restore, not an automatic failover. We publish no uptime SLA, no RPO, and no RTO, and we have not performed a documented restore drill.

Logging and audit

Three separate layers.

1. **Infrastructure.** AWS CloudTrail is enabled account-wide across all regions with log file integrity validation, written to a locked, encrypted bucket with 365-day retention. This covers management events. Object-level S3 access events are not enabled, so there is no storage-layer "who downloaded which file" trail.
2. **Workspace activity.** Team invites and revocations, role changes, user archival and email changes, API key issue and revoke, SSO configuration changes and SSO sign-ins, webhook changes, and billing trial starts are written to an audit log with actor, timestamp, changed fields, and IP address. Workspace administrators can read their own log in the app.
3. **Calibration records.** Every committed calibration is written to an append-only ledger with the recording user and timestamp, chained with SHA-256 so that each record's hash covers the previous record's hash. Attachment file contents are hashed into the chain, not just the file path. Any authenticated user can verify the whole chain from the app.

Scope limit worth stating: edits to an instrument's master record (tag, serial number, calibration interval, location) are not currently written to the workspace activity log. Calibration events themselves are fully covered by the ledger.

Application error monitoring runs through Sentry with personally identifiable information disabled by default and a custom scrubbing hook on every event.

Subprocessors and what each one sees

Party	Role	What it can see
Amazon Web Services (us-east-1)	Hosting, database, storage, email, secrets, logging	All customer data
Stripe	Payment processing	Billing email and a workspace identifier. Card details are entered directly into Stripe and never reach Axiospec servers. No calibration or instrument data.
Sentry	Error and performance monitoring	Stack traces and request paths after scrubbing. Not guaranteed to never contain an identifier that appears in an error message.
Google (Firebase)	Mobile push notifications	Device push tokens, notification content such as calibration-due alerts
Google (OAuth)	Google sign-in	The sign-in event for users who choose it
Google (Analytics 4 / Ads)	Product and marketing analytics	Page paths and interaction events, including inside the signed-in app. No calibration data is transmitted. Consent Mode v2 with regional defaults is implemented.
GitHub	Source control and deployment pipeline	Source code. No customer data.

If you configure outbound webhooks, calibration event data is also sent to the destination **you** choose. That destination is your subprocessor, not ours.

Data ownership and export

Your records are yours. Export is self-service, unlimited, and not gated behind a pricing tier. Managers, administrators, and auditors can generate a complete audit archive at any time.

The archive is a single ZIP containing:

- `audit_manifest.csv`, one row per instrument then one row per committed calibration event, including each record's hash and the previous record's hash in hexadecimal
- `audit_summary.pdf`, a human-readable report with the compliance dashboard, integrity verification result, the full audit trail, the asset roster, and out-of-tolerance details
- the original evidence files, grouped by instrument tag
- a README with the export scope, the first and last record hashes, and a step-by-step procedure to **re-verify the chain linkage yourself, offline, without Axiospec**

Exports can be scoped by site, location, instrument, date range, or compliance status, and the scope can only narrow within your own permissions, never widen. Note that a scoped export verifies each exported record's own hash but does not assert continuity across the whole chain, because it is a deliberate subset. Only a full unscoped export performs the complete chain walk.

Instrument registry data can also be exported to CSV from the browser at any time.

If you stop using Axiospec

Billing stops immediately when you request account closure. Your data is retained for **730 days (about 24 months)** afterward so you can sign back in and export it, and so you can reactivate if you change your mind. After that window it is permanently purged, including the stored evidence files.

There is no export paywall and no proprietary format. Because the audit archive is open-format CSV plus PDF plus your original files plus written instructions for independent chain-linkage verification, the evidence pack remains checkable by a third party even if Axiospec no longer exists.

What we do not have yet

We would rather tell you this up front than have you find it in a questionnaire.

- **No SOC 2 report** (Type I or Type II). No audit has been performed and no auditor is engaged. What we offer instead: this document, direct answers to your questionnaire, and a named contact who responds.
- **No ISO/IEC 27001 certification.** Note that Axiospec supports customers' ISO 9001 and ISO/IEC 17025 programs. That is the product domain and is unrelated to our own information-security certification. We do not blur the two.
- **No third-party penetration test.** Internal review only.
- **No HIPAA BAA, and no FedRAMP, CMMC, NIST 800-171, ITAR, or DFARS 252.204-7012 program.** Do not put protected health information or controlled unclassified information in Axiospec.
- **No multi-factor authentication in the product.** MFA is available today only when you sign in with Google and your Google account enforces it. There is no TOTP, WebAuthn, SMS, or backup-code option in Axiospec itself. Per-tenant enterprise SSO (OIDC and SAML 2.0) is enabled in production. SAML authentication requests are not signed in this version.
- **No published DPA, GDPR terms, Standard Contractual Clauses, or EU data region.** All data is in the United States.
- **No uptime SLA, status page, RPO, or RTO**, and no documented restore drill. Backups are configured; recovery time is not committed.
- **No object versioning on the evidence file bucket.** An overwritten or deleted file has no storage-layer recovery path. The ledger record of the calibration survives regardless.
- **No defined application log retention period.** Application logs currently persist indefinitely by default.
- **No software validation package (IQ/OQ/PQ) and no requirement-to-test traceability matrix.** What we do have: 2,465 test functions across 197 test files that must pass before any production deployment, a dependency vulnerability scan that blocks the build, manual-trigger-only production releases, and immutable per-release images for rollback. That is a real software development control. It is not a validation package, and a computer system validation reviewer should not accept it as one.
- **No least-privilege infrastructure access yet.** Our CI deploy role holds AWS AdministratorAccess. Production deploys are manual-trigger only and gated on a GitHub environment, but anyone who can trigger that workflow has full account administration.

- **No separation of duties or formal access review.** CaliTech LLC is a one-person company. There is no documented personnel security program, background check process, or security training program.
- **No formal written incident response plan, no committed breach-notification window, and no verified cyber liability policy.** Infrastructure alarms are configured in CloudWatch and delivered to an on-call email address. That is monitoring, not a documented IR process.

We are not going to describe any of the above as "in progress" or "aligned with" something we do not hold.

Security contact

Send security questions, questionnaires, or vulnerability reports to **support@axiospec.com**. We reply within one business day. Axiospec is built by CaliTech LLC, Knoxville, Tennessee.

If your review needs an architecture or data-flow diagram, a completed vendor security questionnaire, or a call with the person who wrote the code, ask. You will get all three from the same address.