Axiospec: Sicherheit und Umgang mit Daten

Für IT- und Sicherheitsprüfer. Axiospec ist ein System für Kalibrier- und Messmitteldatensätze, entwickelt von CaliTech LLC, Knoxville, Tennessee (USA). Diese Seite beschreibt, wie der Produktivdienst mit Kundendaten umgeht. Alles Folgende ist eine Aussage über die Produktivumgebung. Zuletzt überprüft: 21. September 2026.

Zwei Dinge vorab. Axiospec besitzt heute keine Sicherheitszertifizierung, und im letzten Abschnitt sagen wir genau, was wir haben und was nicht, statt Sie danach suchen zu lassen. Axiospec ist ein Dokumentationssystem. Es unterstützt und dokumentiert Ihr Kalibrierprogramm und hält es auditbereit. Es zertifiziert, sichert oder garantiert nicht Ihre Konformität mit einer Norm.

Wo Ihre Daten liegen

Amazon Web Services, ein einziges Konto, Region **us-east-1 (Nord-Virginia, USA)**. Jede zustandsbehaftete Produktivressource ist in dieser einen Region deklariert: die PostgreSQL-16-Datenbank, der Bucket für die Dokumentenablage, der Bucket für die Audit-Logs, die Ablage für Geheimnisse und die Rechenleistung der Anwendung.

Das Content Delivery Network vor der Anwendung (Amazon CloudFront) ist ein weltweites Edge-Netzwerk. Es terminiert TLS an einem Edge-Standort, der außerhalb der USA liegen kann, und leitet die Anfrage an us-east-1 weiter. API-Antworten sind ausdrücklich so konfiguriert, dass sie am Edge **nicht** zwischengespeichert werden. Nur statische Ressourcen der Anwendung und der Website werden zwischengespeichert. Die unten aufgeführten Unterauftragsverarbeiter verarbeiten Daten an ihren eigenen Standorten.

Verschlüsselung

Bei der Übertragung. Anwendung und API werden ausschließlich über HTTPS ausgeliefert. Unverschlüsseltes HTTP wird umgeleitet. Die Mindestversion von TLS ist 1.2. Auch die Verbindung vom CDN zurück zur Anwendung nutzt TLS 1.2. Datenbankverbindungen erfordern TLS (`sslmode=require`), und der Authentifizierungsdienst startet nicht mit einer Datenbank-URL, die das nicht verlangt.

Im Ruhezustand. Für die Produktivdatenbank ist die Speicherverschlüsselung aktiviert. Der Bucket für die Audit-Logs der Infrastruktur ist mit SSE-S3 (AES-256) verschlüsselt. Anwendungsgeheimnisse liegen im AWS Secrets Manager und werden zur Laufzeit geladen, statt im Klartext in Umgebungsvariablen zu stehen. Die Nachrichtenwarteschlange für fehlgeschlagene Hintergrundaufgaben nutzt die von SQS verwaltete Verschlüsselung.

Hochgeladene Nachweisdateien (Kalibrierscheine, Fotos) werden in Amazon S3 gespeichert, das Objekte im Ruhezustand standardmäßig mit SSE-S3 verschlüsselt. Diese Einstellung deklarieren wir derzeit nicht ausdrücklich in unserem Infrastrukturcode, daher beschreiben wir sie als Plattformstandard und nicht als

eine von uns nachgewiesene Maßnahme. Die gesamte Verschlüsselung nutzt von AWS verwaltete Schlüssel. Eine Option für vom Kunden verwaltete Schlüssel (BYOK) gibt es nicht.

Netzwerkisolierung

Die Produktivdatenbank ist **nicht öffentlich erreichbar**. Ihre einzige eingehende Regel ist PostgreSQL aus der eigenen Sicherheitsgruppe der Anwendung. Es sind keine IP-Bereiche zugelassen. Der Löschschutz ist aktiviert.

Die Anwendung läuft in einer VPC über zwei Verfügbarkeitszonen in privaten Subnetzen ohne öffentliche IP-Adressen. Ausgehender Verkehr läuft über ein NAT-Gateway; Verkehr zu S3 nutzt einen VPC-Gateway-Endpunkt und läuft nicht über das öffentliche Internet. Die Sicherheitsgruppe der Anwendung hat überhaupt keine eingehenden Regeln.

Bei allen S3-Buckets ist der öffentliche Zugriff in allen vier Einstellungen vollständig gesperrt. Der Bucket der Single-Page-Anwendung ist nur für unsere CloudFront-Distribution lesbar, erzwungen durch Origin Access Control und eine auf diese Distribution beschränkte Bucket-Richtlinie. Der Schreibzugriff der Anwendung auf den Dokumenten-Bucket ist auf `PutObject` und `GetObject` für diesen Bucket beschränkt.

Mandantentrennung

Axiospec ist mandantenfähig: eine gemeinsame Datenbank mit gemeinsamem Schema und **einer zeilenbasierten Mandantenabgrenzung, die die Anwendung erzwingt**. Jede Tabelle mit Kundendaten trägt eine `tenant_id`. Die Mandantenidentität wird aus einem Claim eines signaturgeprüften Tokens gelesen, nie aus einem vom Client gelieferten Header oder Anfragetext. Zentrale Datensatztypen (Messmittel, Journaleinträge, Benutzer) werden zusätzlich durch einen globalen Abfrage-Listener gefiltert, der bei jedem Lesezugriff die Mandantenbedingung einfügt. Hochgeladene Dateien werden unter Objektschlüsseln mit Mandantenpräfix abgelegt.

Genau benannt: Das ist eine von der Anwendung erzwungene Isolierung, keine Sicherheit auf Zeilenebene von PostgreSQL und keine eigene Datenbank oder kein eigenes Schema je Kunde.

Innerhalb eines Arbeitsbereichs gibt es eine zweite Grenze. Standortberechtigungen können einen Benutzer auf bestimmte Werke oder Orte beschränken, und der Server prüft den Standortumfang bei den Vorgängen Erfassen, Freigeben, Stornieren und Exportieren.

Authentifizierung und Zugriffssteuerung

Passwörter werden als PBKDF2-HMAC-SHA256-Hash mit 260.000 Iterationen und einem zufälligen Salt je Passwort gespeichert und in konstanter Zeit geprüft. Die Anmeldung erfolgt entweder mit E-Mail-Adresse und Passwort oder mit der Google-Anmeldung, die in der Produktivumgebung aktiv ist. Über Google angelegte Konten haben kein nutzbares Passwort.

Der Schutz gegen Brute-Force-Angriffe ist eine exponentielle Verzögerung je Konto, die auf Datenbankebene über alle Anwendungsinstanzen geteilt und über einen Hash der Kennung geführt wird, sodass sich ein nicht vorhandenes Konto genauso verhält wie ein echtes. Sie ist gedeckelt, damit sie nicht dazu missbraucht werden kann, Ihre Benutzer auszusperren.

Zwei-Faktor-Authentifizierung ist verfügbar und wird von jedem Benutzer selbst eingerichtet. Es handelt sich um ein zeitbasiertes Einmalpasswort aus einer Authenticator-App, mit einmal verwendbaren Wiederherstellungscodes, die einmal angezeigt und als Hash gespeichert werden, und einem optionalen Token für vertrauenswürdige Geräte, mit dem ein gewähltes Gerät den zweiten Faktor überspringen kann, bis der Token widerrufen wird. Eine Option für WebAuthn, Sicherheitsschlüssel oder SMS gibt es nicht.

Sitzungen nutzen zustandslose signierte Tokens mit einer Standardlaufzeit von 7 Tagen, die im lokalen Speicher des Browsers liegen. Das Deaktivieren oder Löschen eines Benutzers wirkt sofort: Der Kontostatus wird bei jeder Anfrage erneut aus der Datenbank geprüft, sodass ein vorhandener Token beim nächsten Aufruf dieses Benutzers nicht mehr funktioniert. Eine allgemeine Sperrliste gibt es nicht, ein von einem weiterhin aktiven Benutzer gestohlener Token bleibt also bis zu seinem Ablauf gültig.

Die rollenbasierte Zugriffssteuerung wird auf dem Server erzwungen, nicht im Browser. Fünf Rollen: Super-Admin, Administrator, Manager, Techniker, Auditor. Die Rolle wird bei jeder Anfrage erneut aus der Datenbank gelesen, statt dem Token zu vertrauen. Die Auditor-Rolle ist systemweit schreibgeschützt, mit einer eng begrenzten Ausnahme für das Erzeugen eines Auditexports. Manager können Benutzer nicht über ihre eigene Befugnis hinaus befördern.

Zwei Anwendungskontrollen, die für einen Qualitätsprüfer zählen. Festgeschriebene Kalibrierdatensätze können weder bearbeitet noch gelöscht werden, erzwungen durch einen Datenbank-Trigger, sodass das auch bei direktem SQL-Zugriff gilt. Korrekturen werden als neue verknüpfte Datensätze mit einer verpflichtenden schriftlichen Begründung angehängt. Und wenn ein Arbeitsbereich das Vier-Augen-Prinzip aktiviert, lässt das System nicht zu, dass die Person, die eine Kalibrierung erfasst hat, sie auch freigibt.

Die Zugriffskontrollen für die Verwaltungskonsole unseres AWS-Kontos bestätigen wir auf Anfrage gesondert.

Datensicherung und Wiederherstellung

Automatische tägliche Datenbanksicherungen mit **einer Aufbewahrungsfrist von 14 Tagen**, die eine zeitpunktgenaue Wiederherstellung innerhalb dieser Frist ermöglicht. Löschschutz und ein verpflichtender abschließender Snapshot sind aktiviert. Infrastrukturalarme sind in CloudWatch für CPU, Speicher und Verbindungsauslastung der Datenbank, Anwendungsfehler, Drosselung, Latenz, die 5xx-Rate des CDN und fehlgeschlagene Hintergrundaufgaben eingerichtet und gehen an eine E-Mail-Adresse für die Rufbereitschaft.

Ehrliche Grenzen: Die Produktivdatenbank liegt in einer einzigen Verfügbarkeitszone. Ein Ausfall der Zone erfordert eine Wiederherstellung, kein automatisches Failover. Wir veröffentlichen kein Verfügbarkeits-SLA, kein RPO und kein RTO, und wir haben keine dokumentierte Wiederherstellungsübung durchgeführt.

Protokollierung und Audit

Drei getrennte Ebenen.

1. **Infrastruktur.** AWS CloudTrail ist kontoweit in allen Regionen aktiviert, mit Integritätsprüfung der Logdateien, und schreibt in einen gesperrten, verschlüsselten Bucket mit 365 Tagen Aufbewahrung. Das

umfasst Verwaltungsereignisse. Zugriffsereignisse auf S3-Objektebene sind nicht aktiviert, daher gibt es auf Speicherebene keine Spur, wer welche Datei heruntergeladen hat.

2. **Aktivität im Arbeitsbereich.** Teameinladungen und Widerrufe, Rollenänderungen, das Archivieren von Benutzern und Änderungen von E-Mail-Adressen, das Ausstellen und Widerrufen von API-Schlüsseln, Änderungen der SSO-Konfiguration und SSO-Anmeldungen, Webhook-Änderungen sowie der Start von Testphasen in der Abrechnung werden in ein Audit-Log geschrieben, mit handelnder Person, Zeitstempel, geänderten Feldern und IP-Adresse. Administratoren des Arbeitsbereichs können ihr eigenes Log in der Anwendung lesen.
3. **Kalibrierdatensätze.** Jede festgeschriebene Kalibrierung wird in ein Journal geschrieben, an das nur angehängt werden kann, mit erfassendem Benutzer und Zeitstempel, verkettet mit SHA-256, sodass der Hash jedes Datensatzes den Hash des vorherigen Datensatzes einschließt. Der Inhalt angehängter Dateien fließt per Hash in die Kette ein, nicht nur der Dateipfad. Jeder angemeldete Benutzer kann die gesamte Kette in der Anwendung prüfen.

Eine Grenze des Umfangs, die wir nennen wollen: Änderungen am Stammdatensatz eines Messmittels (Kennung, Seriennummer, Kalibrierintervall, Ort) werden derzeit nicht in das Aktivitätsprotokoll des Arbeitsbereichs geschrieben. Die Kalibrierereignisse selbst sind vollständig durch das Journal abgedeckt.

Die Überwachung von Anwendungsfehlern läuft über Sentry, wobei personenbezogene Informationen standardmäßig deaktiviert sind und jedes Ereignis eine eigene Bereinigungsfunktion durchläuft.

Unterauftragsverarbeiter und was jeder sieht

Partei	Aufgabe	Was sie sehen kann
Amazon Web Services (us-east-1)	Hosting, Datenbank, Speicher, E-Mail, Geheimnisse, Protokollierung	Alle Kundendaten
Stripe	Zahlungsabwicklung	Rechnungs-E-Mail-Adresse und eine Kennung des Arbeitsbereichs. Kartendaten werden direkt bei Stripe eingegeben und erreichen die Server von Axiospec nie. Keine Kalibrier- oder Messmitteldaten.
Sentry	Überwachung von Fehlern und Leistung	Stack-Traces und Anfragepfade nach der Bereinigung. Es ist nicht garantiert, dass sie nie eine Kennung enthalten, die in einer Fehlermeldung vorkommt.
Google (Firebase)	Push-Benachrichtigungen auf Mobilgeräten	Push-Tokens der Geräte und der Inhalt der Benachrichtigungen, etwa Hinweise auf fällige Kalibrierungen
Google (Firebase Analytics)	Produktanalyse ausschließlich in der Android-App	Nutzungsereignisse der App und die bei der Anmeldung gesetzte interne Benutzerkennung. Die iOS-App bindet das SDK nicht ein.

Partei	Aufgabe	Was sie sehen kann
Google (Analytics 4)	Produkt- und Webanalyse	Seitenpfade und Interaktionsereignisse, auch in der angemeldeten Anwendung. Es werden keine Kalibrierdaten übertragen. Consent Mode v2 mit regionalen Standardwerten ist umgesetzt. Google Ads wurde am 15. September 2026 eingestellt, und es wird kein Werbe-Tag, keine Werbe-Conversion und kein Remarketing-Pixel ausgeliefert.
Google (OAuth)	Google-Anmeldung	Das Anmeldeereignis der Benutzer, die diese Option wählen
Google (Android-Spracherkennung)	Sprachdiktat von Messwerten in der Android-App	Das diktierte Audio. Es verlässt das Gerät; die Erkennung findet nicht auf dem Gerät statt.
Apple (iOS-Spracherkennung)	Sprachdiktat von Messwerten in der iOS-App	Das diktierte Audio, zu denselben Bedingungen wie bei Android.
GitHub	Quellcodeverwaltung und Deployment-Pipeline	Quellcode. Keine Kundendaten.

Wenn Sie ausgehende Webhooks einrichten, werden Kalibrierereignisdaten auch an das Ziel gesendet, das **Sie** wählen, und diese Nutzlast nennt den Techniker, der die Kalibrierung durchgeführt hat. Dieses Ziel ist Ihr Unterauftragsverarbeiter, nicht unserer.

Dieselbe Liste ist für Kunden unter axiospec.com/subprocessors veröffentlicht, mit dem, was jede Partei erhält und warum. Beide werden im Gleichklang gehalten.

Dateneigentum und Export

Ihre Datensätze gehören Ihnen. Der Export ist Self-Service, unbegrenzt und an keinen Tarif gebunden. Manager, Administratoren und Auditoren können jederzeit ein vollständiges Auditarchiv erzeugen.

Das Archiv ist eine einzige ZIP-Datei mit:

- `audit_manifest.csv`, eine Zeile je Messmittel, danach eine Zeile je festgeschriebenem Kalibrierereignis, einschließlich des Hashes jedes Datensatzes und des Hashes des vorherigen Datensatzes in Hexadezimaldarstellung
- `audit_summary.pdf`, ein lesbarer Bericht mit der Konformitätsübersicht, dem Ergebnis der Integritätsprüfung, dem vollständigen Audit-Trail, dem Messmittelverzeichnis und den Einzelheiten zu Toleranzüberschreitungen
- die ursprünglichen Nachweisdateien, gruppiert nach Messmittelkennung
- eine README mit dem Exportumfang, dem ersten und letzten Datensatz-Hash und einem Schritt-für-Schritt-Verfahren, um **die Verkettung selbst erneut zu prüfen, offline und ohne Axiospec**

Exporte lassen sich nach Standort, Ort, Messmittel, Zeitraum oder Konformitätsstatus eingrenzen, und der Umfang kann innerhalb Ihrer eigenen Berechtigungen nur enger, nie weiter werden. Beachten Sie, dass ein eingegrenzter Export den eigenen Hash jedes exportierten Datensatzes prüft, aber keine Aussage über die

Kontinuität der ganzen Kette trifft, weil er eine bewusst gewählte Teilmenge ist. Nur ein vollständiger Export ohne Umfang durchläuft die gesamte Kette.

Die Daten des Messmittelverzeichnisses lassen sich außerdem jederzeit im Browser als CSV exportieren.

Wenn Sie Axiospec nicht mehr nutzen

Die Abrechnung endet sofort, wenn Sie die Schließung des Kontos beantragen. Ihre Daten werden danach **730 Tage (etwa 24 Monate)** aufbewahrt, damit Sie sich erneut anmelden und sie exportieren können und damit Sie das Konto reaktivieren können, falls Sie es sich anders überlegen. Nach dieser Frist werden sie endgültig gelöscht, einschließlich der gespeicherten Nachweisdateien.

Es gibt keine Bezahlschranke für den Export und kein proprietäres Format. Weil das Auditarchiv aus CSV im offenen Format, PDF, Ihren Originaldateien und einer schriftlichen Anleitung zur unabhängigen Prüfung der Verkettung besteht, bleibt das Nachweispaket für Dritte prüfbar, auch wenn es Axiospec nicht mehr gibt.

Was wir noch nicht haben

Wir sagen Ihnen das lieber vorab, als dass Sie es in einem Fragebogen herausfinden.

- **Kein SOC-2-Bericht** (Typ I oder Typ II). Es wurde kein Audit durchgeführt und kein Prüfer beauftragt. Was wir stattdessen bieten: dieses Dokument, direkte Antworten auf Ihren Fragebogen und einen namentlich benannten Ansprechpartner, der antwortet.
- **Keine Zertifizierung nach ISO/IEC 27001.** Beachten Sie, dass Axiospec die Programme seiner Kunden nach ISO 9001 und ISO/IEC 17025 unterstützt. Das ist die Domäne des Produkts und hat mit unserer eigenen Zertifizierung der Informationssicherheit nichts zu tun. Wir vermischen die beiden nicht.
- **Kein Penetrationstest durch Dritte.** Nur interne Prüfung.
- **Kein HIPAA-BAA und kein Programm für FedRAMP, CMMC, NIST 800-171, ITAR oder DFARS 252.204-7012.** Legen Sie keine geschützten Gesundheitsinformationen und keine kontrollierten, nicht als Verschlusssache eingestuften Informationen in Axiospec ab.
- **Kein zweiter Faktor über WebAuthn, Sicherheitsschlüssel oder SMS.** Die Zwei-Faktor-Authentifizierung in Axiospec ist ein zeitbasiertes Einmalpasswort aus einer Authenticator-App, mit Wiederherstellungscodes und einem optionalen Token für vertrauenswürdige Geräte. Das ist der einzige angebotene zweite Faktor. Mandantenbezogenes Enterprise-SSO (OIDC und SAML 2.0) ist in der Produktivumgebung aktiviert. SAML-Authentifizierungsanfragen werden in dieser Version nicht signiert.
- **Kein veröffentlichter Auftragsverarbeitungsvertrag, keine DSGVO-Bedingungen, keine Standardvertragsklauseln und keine EU-Datenregion.** Alle Daten liegen in den USA, in us-east-1. Entwürfe eines Auftragsverarbeitungsvertrags und von Übermittlungsbedingungen liegen vor und befinden sich bei unseren Anwälten. Nichts davon ist in Kraft, und wir werden einen Entwurf nicht so beschreiben, als wäre er es.
- **Kein Verfügbarkeits-SLA, keine Statusseite, kein RPO oder RTO** und keine dokumentierte Wiederherstellungsübung. Sicherungen sind eingerichtet; eine Wiederherstellungszeit sagen wir nicht zu.
- **Keine Objektversionierung im Bucket für Nachweisdateien.** Eine überschriebene oder gelöschte Datei hat auf Speicherebene keinen Wiederherstellungsweg. Der Journaleintrag der Kalibrierung bleibt in

jedem Fall erhalten.

- **Keine festgelegte Aufbewahrungsfrist für Anwendungslogs.** Anwendungslogs bleiben derzeit standardmäßig unbegrenzt erhalten.
- **Kein Softwarevalidierungspaket (IQ/OQ/PQ) und keine Rückverfolgbarkeitsmatrix von Anforderungen zu Tests.** Was wir haben: 2.465 Testfunktionen in 197 Testdateien, die vor jedem Produktiv-Deployment bestanden sein müssen, eine Schwachstellenprüfung der Abhängigkeiten, die den Build blockiert, Produktivreleases nur auf manuellen Auslöser und unveränderliche Images je Release für den Rollback. Das ist eine echte Kontrolle der Softwareentwicklung. Es ist kein Validierungspaket, und ein Prüfer für die Validierung computergestützter Systeme sollte es nicht als solches akzeptieren.
- **Noch kein Infrastrukturzugriff nach dem Prinzip der minimalen Rechte.** Unsere CI-Deployment-Rolle hat AWS AdministratorAccess. Produktiv-Deployments werden nur manuell ausgelöst und sind über eine GitHub-Umgebung abgesichert, aber wer diesen Workflow auslösen kann, hat die vollständige Kontoverwaltung.
- **Keine Funktionstrennung und keine formale Überprüfung von Zugriffsrechten.** CaliTech LLC ist ein Ein-Personen-Unternehmen. Es gibt kein dokumentiertes Programm zur personellen Sicherheit, kein Verfahren zur Hintergrundprüfung und kein Schulungsprogramm zur Sicherheit.
- **Kein vollständiger Plan zur Reaktion auf Vorfälle und keine geprüfte Cyber-Versicherung.** Was es seit dem 21. September 2026 gibt, ist ein schriftliches Ablaufhandbuch für die Meldung von Datenschutzverletzungen: was als Verletzung des Schutzes personenbezogener Daten gilt, wer entscheidet, die 72-Stunden-Frist und wer in welcher Reihenfolge informiert wird. Es ist ein internes Dokument und wurde noch in keiner Übung erprobt. Infrastrukturalarme sind in CloudWatch eingerichtet und gehen an eine E-Mail-Adresse für die Rufbereitschaft; das ist Überwachung, kein Reaktionsprozess.

Wir werden nichts davon als "in Arbeit" oder als "ausgerichtet an" etwas beschreiben, das wir nicht besitzen.

Ansprechpartner für Sicherheit

Senden Sie Sicherheitsfragen, Fragebögen oder Meldungen zu Schwachstellen an **support@axiospec.com**. Wir antworten innerhalb eines Werktags. Axiospec wird von CaliTech LLC, Knoxville, Tennessee (USA), entwickelt.

Wenn Ihre Prüfung ein Architektur- oder Datenflussdiagramm, einen ausgefüllten Sicherheitsfragebogen für Lieferanten oder ein Gespräch mit der Person braucht, die den Code geschrieben hat, fragen Sie danach. Sie erhalten alle drei über dieselbe Adresse.