Axiospec : sécurité et traitement des données

Pour les équipes des TI et les évaluateurs en sécurité. Axiospec est un système de dossiers d'étalonnage et d'actifs développé par CaliTech LLC, Knoxville, au Tennessee (États-Unis). Cette page décrit la façon dont le service de production traite les données des clients. Tout ce qui suit est un énoncé qui porte sur la production. Dernière révision : le 21 septembre 2026.

Deux choses à savoir avant d'aller plus loin. Axiospec ne détient aujourd'hui aucune certification de sécurité, et nous disons exactement ce que nous avons et ce que nous n'avons pas dans la dernière section, plutôt que de vous obliger à le chercher. Axiospec est un système de gestion documentaire. Il soutient et documente votre programme d'étalonnage et le garde prêt pour l'audit. Il ne certifie, n'assure ni ne garantit votre conformité à aucune norme.

Où se trouvent vos données

Amazon Web Services, un seul compte, région **us-east-1 (Virginie du Nord, États-Unis)**. Toutes les ressources de production avec état sont déclarées dans cette seule région : la base de données PostgreSQL 16, le compartiment de stockage des documents, le compartiment des journaux d'audit, le stockage des secrets et le calcul de l'application.

Le réseau de diffusion de contenu placé devant l'application (Amazon CloudFront) est un réseau périphérique mondial. Il termine le TLS dans un emplacement périphérique qui peut se trouver à l'extérieur des États-Unis et achemine la requête vers us-east-1. Les réponses de l'API sont explicitement configurées pour **ne pas** être mises en cache en périphérie. Seules les ressources statiques de l'application et du site Web sont mises en cache. Les sous-traitants énumérés plus bas traitent les données dans leurs propres emplacements.

Chiffrement

En transit. L'application et l'API sont servies uniquement en HTTPS. Le HTTP non chiffré est redirigé. La version minimale de TLS est la 1.2. La connexion du CDN vers l'application utilise elle aussi TLS 1.2. Les connexions à la base de données exigent TLS (`sslmode=require`), et le service d'authentification refuse de démarrer avec une URL de base de données qui ne l'exige pas.

Au repos. Le chiffrement du stockage est activé sur la base de données de production. Le compartiment des journaux d'audit de l'infrastructure est chiffré avec SSE-S3 (AES-256). Les secrets de l'application sont conservés dans AWS Secrets Manager et chargés à l'exécution, plutôt que de se trouver en clair dans des variables d'environnement. La file de messages utilisée pour les tâches d'arrière-plan en échec utilise le chiffrement géré par SQS.

Les fichiers de preuve téléversés (certificats d'étalonnage, photos) sont stockés dans Amazon S3, qui chiffre par défaut les objets au repos avec SSE-S3. Nous ne déclarons pas actuellement ce paramètre de

façon explicite dans notre code d'infrastructure, alors nous le décrivons comme le comportement par défaut de la plateforme et non comme une mesure dont nous faisons la preuve. Tout le chiffrement utilise des clés gérées par AWS. Il n'existe aucune option de clés gérées par le client (BYOK).

Isolement réseau

La base de données de production **n'est pas accessible publiquement**. Sa seule règle entrante est PostgreSQL à partir du propre groupe de sécurité de l'application. Aucune plage d'adresses IP n'est permise. La protection contre la suppression est activée.

L'application s'exécute dans un VPC, sur deux zones de disponibilité, dans des sous-réseaux privés sans adresse IP publique. Le trafic sortant passe par une passerelle NAT; le trafic vers S3 utilise un point de terminaison de passerelle VPC et ne passe pas par Internet. Le groupe de sécurité de l'application n'a aucune règle entrante.

L'accès public est entièrement bloqué sur les quatre paramètres pour tous les compartiments S3. Le compartiment de l'application monopage n'est lisible que par notre distribution CloudFront, ce qu'imposent Origin Access Control et une politique de compartiment limitée à cette distribution. L'accès en écriture de l'application au compartiment des documents se limite à `PutObject` et `GetObject` sur ce compartiment.

Séparation des clients

Axiospec est multilocataire : une base de données partagée, un schéma partagé et **un cloisonnement par locataire au niveau des lignes, imposé dans l'application**. Chaque table qui contient des données de clients porte un `tenant_id`. L'identité du locataire est lue dans une revendication d'un jeton dont la signature est vérifiée, jamais dans un en-tête ou un corps de requête fournis par le client. Les principaux types d'enregistrements (instruments, entrées du registre, utilisateurs) sont en plus filtrés par un listener global de requêtes qui injecte la condition du locataire à chaque lecture. Les fichiers téléversés sont stockés sous des clés d'objet préfixées par le locataire.

Soyons précis sur ce que c'est : il s'agit d'un isolement imposé par l'application, pas de la sécurité au niveau des lignes de PostgreSQL, ni d'une base de données ou d'un schéma distincts par client.

À l'intérieur d'un espace de travail, il existe une deuxième frontière. Les droits par site peuvent limiter un utilisateur à des usines ou à des emplacements précis, et le serveur vérifie la portée du site lors des opérations d'enregistrement, d'approbation, d'annulation et d'exportation.

Authentification et contrôle d'accès

Les mots de passe sont stockés sous forme d'empreinte PBKDF2-HMAC-SHA256 avec 260 000 itérations et un sel aléatoire par mot de passe, et vérifiés en temps constant. La connexion se fait avec une adresse courriel et un mot de passe, ou avec la connexion Google, qui est active en production. Les comptes créés par Google n'ont pas de mot de passe utilisable.

La protection contre les attaques par force brute est un délai exponentiel par compte, partagé entre toutes les instances de l'application au niveau de la base de données et calculé à partir d'une empreinte de

l'identifiant, de sorte qu'un compte inexistant se comporte exactement comme un vrai. Il est plafonné pour ne pas pouvoir servir à un déni de service contre vos utilisateurs.

L'authentification à deux facteurs est offerte et chaque utilisateur l'active lui-même. Il s'agit d'un mot de passe à usage unique basé sur le temps, fourni par une application d'authentification, avec des codes de récupération à usage unique affichés une seule fois et stockés sous forme d'empreinte, ainsi qu'un jeton facultatif d'appareil de confiance qui permet à un appareil choisi de sauter le deuxième facteur jusqu'à ce qu'il soit révoqué. Il n'y a pas d'option WebAuthn, clé de sécurité ou texto.

Les sessions utilisent des jetons signés sans état, d'une durée de validité par défaut de 7 jours, conservés dans le stockage local du navigateur. La désactivation ou la suppression d'un utilisateur prend effet immédiatement : l'état du compte est revérifié dans la base de données à chaque requête, alors un jeton existant cesse de fonctionner au prochain appel de cet utilisateur. Il n'existe pas de liste de révocation générale, donc un jeton volé à un utilisateur toujours actif reste valide jusqu'à son expiration.

Le contrôle d'accès fondé sur les rôles est imposé sur le serveur, pas dans le navigateur. Cinq rôles : super-administrateur, administrateur, gestionnaire, technicien, auditeur. Le rôle est relu dans la base de données à chaque requête plutôt que d'être tiré du jeton. Le rôle d'auditeur est imposé en lecture seule dans tout le système, avec une seule exception étroite pour générer une exportation d'audit. Les gestionnaires ne peuvent pas promouvoir des utilisateurs au-delà de leur propre autorité.

Deux contrôles de l'application qui comptent pour un évaluateur de la qualité. Les enregistrements d'étalonnage confirmés ne peuvent être ni modifiés ni supprimés, ce qu'impose un déclencheur de la base de données; cela tient donc même en cas d'accès SQL direct. Les corrections sont ajoutées comme de nouveaux enregistrements liés, avec un motif écrit obligatoire. Et quand un espace de travail active la révision rédacteur-réviseur, le système refuse que la personne qui a enregistré un étalonnage l'approuve.

Les contrôles d'accès à la console d'administration de notre compte AWS sont confirmés séparément, sur demande.

Sauvegardes et reprise

Sauvegardes quotidiennes automatiques de la base de données avec **une période de conservation de 14 jours**, qui permet une restauration à un moment précis à l'intérieur de cette période. La protection contre la suppression et un instantané final obligatoire sont activés. Des alarmes d'infrastructure sont configurées dans CloudWatch pour le processeur, le stockage et la saturation des connexions de la base de données, les erreurs de l'application, la limitation de débit, la latence, le taux d'erreurs 5xx du CDN et les tâches d'arrière-plan en échec; elles sont envoyées à une adresse courriel de garde.

Limites, en toute honnêteté : la base de données de production se trouve dans une seule zone de disponibilité. Une panne de cette zone exige une restauration, pas un basculement automatique. Nous ne publions aucune entente de niveau de service (SLA) sur la disponibilité, aucun RPO et aucun RTO, et nous n'avons fait aucun exercice de restauration documenté.

Journalisation et audit

Trois couches distinctes.

1. **Infrastructure.** AWS CloudTrail est activé sur tout le compte et dans toutes les régions, avec validation de l'intégrité des fichiers journaux, et écrit dans un compartiment verrouillé et chiffré avec une conservation de 365 jours. Cela couvre les événements de gestion. Les événements d'accès au niveau des objets S3 ne sont pas activés, donc il n'existe aucune trace au niveau du stockage indiquant « qui a téléchargé quel fichier ».
2. **Activité de l'espace de travail.** Les invitations et révocations de l'équipe, les changements de rôle, l'archivage d'utilisateurs et les changements d'adresse courriel, l'émission et la révocation de clés d'API, les modifications de la configuration SSO et les connexions SSO, les modifications de webhooks et les débuts de période d'essai de la facturation sont écrits dans un journal d'audit avec l'auteur, l'horodatage, les champs modifiés et l'adresse IP. Les administrateurs de l'espace de travail peuvent consulter leur propre journal dans l'application.
3. **Dossiers d'étalonnage.** Chaque étalonnage confirmé est écrit dans un registre en ajout seulement, avec l'utilisateur qui l'a enregistré et l'horodatage, enchaîné en SHA-256 de sorte que l'empreinte de chaque enregistrement couvre l'empreinte de l'enregistrement précédent. Le contenu des fichiers joints est intégré à la chaîne par son empreinte, pas seulement le chemin du fichier. Tout utilisateur authentifié peut vérifier la chaîne complète dans l'application.

Une limite de portée à signaler : les modifications de la fiche maître d'un instrument (étiquette, numéro de série, intervalle d'étalonnage, emplacement) ne sont pas encore écrites dans le journal d'activité de l'espace de travail. Les événements d'étalonnage eux-mêmes sont entièrement couverts par le registre.

La surveillance des erreurs de l'application passe par Sentry, avec les renseignements personnels désactivés par défaut et une fonction de nettoyage maison appliquée à chaque événement.

Sous-traitants et ce que chacun voit

Tiers	Rôle	Ce qu'il peut voir
Amazon Web Services (us-east-1)	Hébergement, base de données, stockage, courriel, secrets, journalisation	Toutes les données des clients
Stripe	Traitement des paiements	L'adresse courriel de facturation et un identifiant d'espace de travail. Les données de carte sont saisies directement chez Stripe et n'atteignent jamais les serveurs d'Axiospec. Aucune donnée d'étalonnage ni d'instrument.
Sentry	Surveillance des erreurs et du rendement	Traces d'appels et chemins de requête après nettoyage. Rien ne garantit qu'elles ne contiennent jamais un identifiant présent dans un message d'erreur.
Google (Firebase)	Notifications poussées sur mobile	Jetons de notification des appareils et contenu des notifications, comme les alertes d'étalonnage à échéance

Tiers	Rôle	Ce qu'il peut voir
Google (Firebase Analytics)	Analyse de produit seulement dans l'application Android	Événements d'utilisation de l'application et identifiant interne de l'utilisateur défini à la connexion. L'application iOS n'intègre pas la trousse de développement (SDK).
Google (Analytics 4)	Analyse de produit et Web	Chemins de page et événements d'interaction, y compris dans l'application connectée. Aucune donnée d'étalonnage n'est transmise. Consent Mode v2 avec des valeurs par défaut régionales est en place. Google Ads a été abandonné le 15 septembre 2026, et aucune balise publicitaire, conversion publicitaire ni pixel de reciblage n'est diffusé.
Google (OAuth)	Connexion Google	L'événement de connexion des utilisateurs qui la choisissent
Google (reconnaissance vocale Android)	Dictée vocale des lectures dans l'application Android	L'audio dicté. Il quitte l'appareil; la reconnaissance ne se fait pas sur l'appareil.
Apple (reconnaissance vocale iOS)	Dictée vocale des lectures dans l'application iOS	L'audio dicté, aux mêmes conditions que sur Android.
GitHub	Gestion du code source et chaîne de déploiement	Code source. Aucune donnée de client.

Si vous configurez des webhooks sortants, les données des événements d'étalonnage sont aussi envoyées à la destination que **vous** choisissez, et ce contenu nomme le technicien qui a effectué l'étalonnage. Cette destination est votre sous-traitant, pas le nôtre.

La même liste est publiée pour les clients à axiospec.com/subprocessors, avec ce que chaque tiers reçoit et pourquoi. Les deux sont maintenues en phase.

Propriété et exportation des données

Vos dossiers vous appartiennent. L'exportation est en libre-service, illimitée et n'est liée à aucun forfait. Les gestionnaires, administrateurs et auditeurs peuvent générer à tout moment une archive d'audit complète.

L'archive est un seul fichier ZIP qui contient :

- `audit_manifest.csv`, une ligne par instrument puis une ligne par événement d'étalonnage confirmé, y compris l'empreinte de chaque enregistrement et l'empreinte de l'enregistrement précédent en hexadécimal
- `audit_summary.pdf`, un rapport lisible avec le tableau de bord de conformité, le résultat de la vérification d'intégrité, la piste d'audit complète, le registre des actifs et le détail des cas hors tolérance
- les fichiers de preuve d'origine, regroupés par étiquette d'instrument
- un README indiquant la portée de l'exportation, la première et la dernière empreinte d'enregistrement, et une procédure étape par étape pour **revérifier vous-même l'enchaînement de la chaîne, hors ligne et**

sans Axiospec

Les exportations peuvent être limitées par site, emplacement, instrument, période ou statut de conformité, et la portée peut seulement se resserrer à l'intérieur de vos propres droits, jamais s'élargir. Notez qu'une exportation limitée vérifie l'empreinte propre à chaque enregistrement exporté, mais n'affirme pas la continuité de toute la chaîne, puisqu'il s'agit d'un sous-ensemble délibéré. Seule une exportation complète, sans portée, parcourt la chaîne entière.

Les données du registre des instruments peuvent aussi être exportées en CSV à partir du navigateur en tout temps.

Si vous cessez d'utiliser Axiospec

La facturation s'arrête immédiatement quand vous demandez la fermeture du compte. Vos données sont ensuite conservées **730 jours (environ 24 mois)**, pour que vous puissiez vous reconnecter et les exporter, et pour que vous puissiez réactiver le compte si vous changez d'idée. Après cette période, elles sont purgées de façon permanente, y compris les fichiers de preuve stockés.

Il n'y a ni exportation payante ni format propriétaire. Comme l'archive d'audit se compose de CSV en format ouvert, de PDF, de vos fichiers d'origine et d'instructions écrites pour vérifier de façon indépendante l'enchaînement de la chaîne, un tiers peut toujours vérifier le dossier de preuves même si Axiospec n'existe plus.

Ce que nous n'avons pas encore

Nous préférons vous le dire d'emblée plutôt que vous le laisser découvrir dans un questionnaire.

- **Aucun rapport SOC 2** (Type I ou Type II). Aucun audit n'a été réalisé et aucun auditeur n'a été mandaté. Ce que nous offrons à la place : ce document, des réponses directes à votre questionnaire et une personne-ressource nommée qui répond.
- **Aucune certification ISO/IEC 27001.** Notez qu'Axiospec soutient les programmes ISO 9001 et ISO/IEC 17025 de ses clients. C'est le domaine du produit, sans lien avec notre propre certification en sécurité de l'information. Nous ne confondons pas les deux.
- **Aucun test d'intrusion réalisé par un tiers.** Révision interne seulement.
- **Aucune entente BAA au sens de la HIPAA, et aucun programme FedRAMP, CMMC, NIST 800-171, ITAR ou DFARS 252.204-7012.** Ne versez pas de renseignements de santé protégés ni de renseignements non classifiés contrôlés dans Axiospec.
- **Aucun deuxième facteur WebAuthn, clé de sécurité ou texto.** L'authentification à deux facteurs d'Axiospec est un mot de passe à usage unique basé sur le temps, fourni par une application d'authentification, avec des codes de récupération et un jeton facultatif d'appareil de confiance. C'est le seul deuxième facteur offert. L'authentification unique (SSO) d'entreprise par locataire (OIDC et SAML 2.0) est activée en production. Les requêtes d'authentification SAML ne sont pas signées dans cette version.
- **Aucune entente de traitement des données (DPA) publiée, aucune condition RGPD, aucune clause contractuelle type ni région de données dans l'UE.** Toutes les données se trouvent aux États-Unis,

dans us-east-1. Des ébauches d'une entente de traitement des données et de conditions de transfert existent et sont entre les mains de nos avocats. Rien n'est en vigueur, et nous ne présenterons pas une ébauche comme si elle l'était.

- **Aucune entente de niveau de service (SLA) sur la disponibilité, aucune page d'état, aucun RPO ni RTO**, et aucun exercice de restauration documenté. Les sauvegardes sont configurées; le délai de reprise n'est pas garanti.
- **Aucune gestion des versions des objets dans le compartiment des fichiers de preuve.** Un fichier écrasé ou supprimé n'a aucune voie de récupération au niveau du stockage. L'enregistrement de l'étalonnage dans le registre subsiste dans tous les cas.
- **Aucune période de conservation définie pour les journaux de l'application.** Les journaux de l'application sont actuellement conservés indéfiniment par défaut.
- **Aucun dossier de validation du logiciel (IQ/OQ/PQ) et aucune matrice de traçabilité des exigences vers les tests.** Ce que nous avons : 2 465 fonctions de test réparties dans 197 fichiers de test, qui doivent réussir avant tout déploiement en production, une analyse des vulnérabilités des dépendances qui bloque la compilation, des mises en production déclenchées uniquement à la main, et des images immuables par version pour revenir en arrière. C'est une vraie mesure de contrôle du développement logiciel. Ce n'est pas un dossier de validation, et un évaluateur en validation de systèmes informatisés ne devrait pas l'accepter comme tel.
- **Pas encore d'accès à l'infrastructure selon le principe du moindre privilège.** Notre rôle de déploiement CI détient AWS AdministratorAccess. Les déploiements en production sont déclenchés uniquement à la main et protégés par un environnement GitHub, mais toute personne qui peut déclencher ce flux de travail dispose de l'administration complète du compte.
- **Aucune séparation des tâches ni revue formelle des accès.** CaliTech LLC est une entreprise d'une seule personne. Il n'existe aucun programme documenté de sécurité du personnel, aucune procédure de vérification des antécédents ni aucun programme de formation en sécurité.
- **Aucun plan complet d'intervention en cas d'incident et aucune police d'assurance cyberrisques vérifiée.** Ce qui existe, depuis le 21 septembre 2026, est une procédure écrite de notification des atteintes : ce qui constitue une atteinte aux renseignements personnels, qui décide, le délai de 72 heures, et qui est avisé dans quel ordre. C'est un document interne, qui n'a pas encore été mis à l'essai lors d'un exercice. Des alarmes d'infrastructure sont configurées dans CloudWatch et envoyées à une adresse courriel de garde, ce qui relève de la surveillance et non d'un processus d'intervention.

Nous ne présenterons rien de ce qui précède comme « en cours » ni comme « aligné sur » quelque chose que nous ne détenons pas.

Personne-ressource en sécurité

Envoyez vos questions de sécurité, vos questionnaires ou vos signalements de vulnérabilités à **support@axiospec.com**. Nous répondons en un jour ouvrable. Axiospec est développé par CaliTech LLC, Knoxville, au Tennessee (États-Unis).

Si votre évaluation exige un schéma d'architecture ou de flux de données, un questionnaire de sécurité des fournisseurs rempli ou un appel avec la personne qui a écrit le code, demandez-le. Vous obtiendrez les trois à la même adresse.

Axiospec est publié par CaliTech LLC, Knoxville, Tennessee (États-Unis). Axiospec soutient et documente votre programme d'étalonnage et le garde prêt pour l'audit. Il ne certifie, n'assure ni ne garantit la conformité à aucune norme; cette détermination vous revient, à vous et à votre auditeur. Questions : support@axiospec.com