Axiospec : sécurité et traitement des données

Pour les équipes informatiques et les évaluateurs sécurité. Axiospec est un système d'enregistrement des étalonnages et des équipements développé par CaliTech LLC, Knoxville, Tennessee (États-Unis). Cette page décrit la façon dont le service de production traite les données des clients. Tout ce qui suit est une affirmation sur la production. Dernière revue : 21 septembre 2026.

Deux choses à savoir avant d'aller plus loin. Axiospec ne détient aujourd'hui aucune certification de sécurité, et nous disons précisément 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 maintient 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 compte unique, 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 bucket de stockage des documents, le bucket 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 point de présence qui peut se trouver hors des États-Unis et transmet la requête à 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 sont mises en cache. Les sous-traitants listés plus bas traitent les données dans leurs propres implantations.

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 bucket 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, au lieu de figurer 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 envoyés (certificats d'étalonnage, photos) sont stockés dans Amazon S3, qui chiffre par défaut les objets au repos avec SSE-S3. Nous ne déclarons pas aujourd'hui ce paramètre de façon explicite dans notre code d'infrastructure, nous le décrivons donc comme le comportement par défaut de la

plateforme et non comme une mesure que nous prouvons. Tout le chiffrement utilise des clés gérées par AWS. Il n'existe pas d'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 depuis le propre groupe de sécurité de l'application. Aucune plage d'adresses IP n'est autorisée. 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 transite pas par l'internet public. 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 buckets S3. Le bucket de l'application monopage n'est lisible que par notre distribution CloudFront, ce qu'imposent Origin Access Control et une stratégie de bucket limitée à cette distribution. L'accès en écriture de l'application au bucket des documents est limité à `PutObject` et `GetObject` sur ce bucket.

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 contenant des données 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 outre filtrés par un listener global de requêtes qui injecte la condition du locataire à chaque lecture. Les fichiers envoyés sont stockés sous des clés d'objet préfixées par le locataire.

Soyons exacts 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 seconde frontière. Les droits par site peuvent limiter un utilisateur à des usines ou des emplacements précis, et le serveur vérifie le périmètre de site pour les opérations d'enregistrement, d'approbation, d'annulation et d'export.

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 soit par adresse e-mail et mot de passe, soit par la connexion Google, qui est active en production. Les comptes créés via Google n'ont pas de mot de passe utilisable.

La protection contre la force brute est un délai exponentiel par compte, partagé entre toutes les instances de l'application au niveau de la base de données et indexé sur une empreinte de l'identifiant, de sorte qu'un compte inexistant se comporte exactement comme un compte réel. Il est plafonné pour ne pas pouvoir être retourné en déni de service contre vos utilisateurs.

L'authentification à deux facteurs est disponible 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, et un jeton facultatif d'appareil de confiance qui permet à un appareil choisi de se passer du second facteur jusqu'à sa révocation. Il n'existe pas d'option WebAuthn, clé de sécurité ou SMS.

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, si bien qu'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, responsable, technicien, auditeur. Le rôle est relu dans la base de données à chaque requête au lieu de faire confiance au jeton. Le rôle d'auditeur est imposé en lecture seule dans tout le système, avec une seule exception étroite pour générer un export d'audit. Les responsables ne peuvent pas promouvoir des utilisateurs au-delà de leur propre autorité.

Deux contrôles applicatifs qui comptent pour un évaluateur qualité. Les enregistrements d'étalonnage confirmés ne peuvent être ni modifiés ni supprimés, ce qu'impose un trigger de la base de données ; cela vaut donc même en cas d'accès SQL direct. Les corrections sont ajoutées comme de nouveaux enregistrements liés, avec un motif écrit obligatoire. Et lorsqu'un espace de travail active la revue par un auteur puis un vérificateur, 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 durée de conservation de 14 jours**, qui permet une restauration à un instant donné dans cette fenêtre. 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 applicatives, 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 e-mail d'astreinte.

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 une bascule automatique. Nous ne publions ni SLA de disponibilité, ni RPO, ni RTO, et nous n'avons pas réalisé d'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 bucket 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, il n'existe donc pas de 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 e-mail, 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 lire leur propre journal dans l'application.
3. **Enregistrements d'étalonnage.** Chaque étalonnage confirmé est écrit dans un registre en ajout seul, avec l'utilisateur qui l'a enregistré et l'horodatage, chaîné en SHA-256 de sorte que l'empreinte de chaque enregistrement couvre l'empreinte de l'enregistrement précédent. Le contenu des fichiers joints entre dans la chaîne par son empreinte, pas seulement le chemin du fichier. Tout utilisateur authentifié peut vérifier l'ensemble de la chaîne depuis l'application.

Une limite de périmètre à signaler : les modifications de la fiche principale d'un instrument (repère, 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 applicatives passe par Sentry, avec les informations personnelles identifiantes désactivées par défaut et une fonction de nettoyage propre 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, e-mail, secrets, journalisation	Toutes les données clients
Stripe	Traitement des paiements	L'adresse e-mail 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 des performances	Traces d'appels et chemins de requête après nettoyage. Il n'est pas garanti qu'elles ne contiennent jamais un identifiant présent dans un message d'erreur.
Google (Firebase)	Notifications push sur mobile	Jetons push des appareils et contenu des notifications, comme les alertes d'étalonnage à échéance
Google (Firebase Analytics)	Analyse produit uniquement 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 le SDK.

Tiers	Rôle	Ce qu'il peut voir
Google (Analytics 4)	Analyse 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 remarketing n'est diffusé.
Google (OAuth)	Connexion Google	L'événement de connexion des utilisateurs qui la choisissent
Google (reconnaissance vocale Android)	Dictée vocale des relevés 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 relevés dans l'application iOS	L'audio dicté, dans les mêmes conditions que sur Android.
GitHub	Gestion du code source et chaîne de déploiement	Code source. Aucune donnée client.

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

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

Propriété et export des données

Vos enregistrements vous appartiennent. L'export est en libre-service, illimité et ne dépend d'aucune formule tarifaire. Les responsables, administrateurs et auditeurs peuvent générer à tout moment une archive d'audit complète.

L'archive est un fichier ZIP unique 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 équipements et le détail des hors tolérance
- les fichiers de preuve d'origine, regroupés par repère d'instrument
- un README indiquant le périmètre de l'export, la première et la dernière empreinte d'enregistrement, et une procédure pas à pas pour **revérifier vous-même le chaînage, hors ligne et sans Axiospec**

Les exports peuvent être restreints par site, emplacement, instrument, plage de dates ou statut de conformité, et le périmètre ne peut que se resserrer à l'intérieur de vos propres droits, jamais s'élargir.

Notez qu'un export restreint 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. Seul un export complet, sans périmètre, parcourt toute la chaîne.

Les données du registre des instruments peuvent aussi être exportées en CSV depuis le navigateur à tout moment.

Si vous cessez d'utiliser Axiospec

La facturation s'arrête immédiatement lorsque 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'avis. Passé ce délai, elles sont définitivement purgées, y compris les fichiers de preuve stockés.

Il n'y a ni export payant 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 le chaînage de façon indépendante, le dossier de preuves reste vérifiable par un tiers 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'est mandaté. Ce que nous proposons à la place : ce document, des réponses directes à votre questionnaire et un interlocuteur nommé 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 rapport avec notre propre certification en sécurité de l'information. Nous ne confondons pas les deux.
- **Aucun test d'intrusion réalisé par un tiers.** Revue interne uniquement.
- **Aucun BAA HIPAA, ni aucun programme FedRAMP, CMMC, NIST 800-171, ITAR ou DFARS 252.204-7012.** Ne placez pas d'informations de santé protégées ni d'informations non classifiées contrôlées dans Axiospec.
- **Aucun second facteur WebAuthn, clé de sécurité ou SMS.** 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 second facteur proposé. Le SSO d'entreprise par locataire (OIDC et SAML 2.0) est activé en production. Les requêtes d'authentification SAML ne sont pas signées dans cette version.
- **Aucun DPA publié, 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 projets d'accord 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 un projet comme s'il l'était.
- **Aucun SLA de disponibilité, page d'état, RPO ou RTO**, et aucun exercice de restauration documenté. Les sauvegardes sont configurées ; le délai de reprise n'est pas garanti.

- **Aucun versionnage des objets sur le bucket des fichiers de preuve.** Un fichier écrasé ou supprimé n'a pas de voie de récupération au niveau du stockage. L'enregistrement de l'étalonnage dans le registre subsiste dans tous les cas.
- **Aucune durée de conservation définie pour les journaux applicatifs.** Les journaux applicatifs sont aujourd'hui 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 uniquement sur déclenchement manuel, et des images immuables par version pour revenir en arrière. C'est une vraie mesure de maîtrise 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 moindre privilège.** Notre rôle de déploiement CI dispose d'AWS AdministratorAccess. Les déploiements en production sont déclenchés uniquement à la main et protégés par un environnement GitHub, mais toute personne pouvant déclencher ce workflow 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 pas de programme documenté de sécurité du personnel, de procédure de vérification des antécédents ni de programme de formation à la sécurité.
- **Aucun plan complet de réponse aux incidents et aucune police cyber-assurance vérifiée.** Ce qui existe, depuis le 21 septembre 2026, est une procédure écrite de notification des violations : ce qui constitue une violation de données personnelles, qui décide, le délai de 72 heures, et qui est prévenu dans quel ordre. C'est un document interne, qui n'a pas encore été éprouvé lors d'un exercice. Des alarmes d'infrastructure sont configurées dans CloudWatch et envoyées à une adresse e-mail d'astreinte, ce qui relève de la surveillance et non d'un processus de réponse.

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

Contact sécurité

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

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