Architecture, hébergement et sécurité

Ce dossier répond aux questions qu'une direction des systèmes d'information pose avant d'ouvrir un service à ses équipes : où vivent les données, qui peut les lire, comment le service s'intègre à l'existant, et ce qui se passe le jour où quelque chose casse. Les engagements cités sont repris à l'identique dans le contrat de licence.

L'ARCHITECTURE — TROIS NIVEAUX, AUCUN AGENT À DÉPLOYER

01
Postes et mobiles
Un navigateur, rien d'autre

Application web progressive. Aucun client lourd, aucun agent, aucun paquet à pousser par Intune. La saisie terrain continue de fonctionner hors couverture réseau et se synchronise au retour du signal.

02
Application
Région Paris

Rendu et actions exécutés côté serveur, sur une plateforme d'exécution managée épinglée à la région Paris. Aucune décision de sécurité n'est laissée au navigateur.

03
Données
Instance dédiée

Base PostgreSQL managée, comptes, sessions et fichiers. Une instance par client : aucune donnée de deux laboratoires ne cohabite dans une même base.

04
Réseau
TLS 1.3 de bout en bout

Chiffrement sur toutes les liaisons, imposé par en-tête pour deux ans et préchargé dans les navigateurs. Aucun port à ouvrir chez vous, aucun flux entrant vers votre réseau.

OÙ VIVENT LES DONNÉES ET QUI LES TRAITE

SOUS-TRAITANT	RÔLE DANS LE TRAITEMENT	LOCALISATION	GARANTIES
Vercel Exécution	Hébergement du code et des fonctions serveur de l'application. Aucune donnée métier n'est stockée à ce niveau : le calcul y passe, la donnée non.	France — région Paris	SOC 2 Type II · ISO 27001 Accord de sous-traitance art. 28
Supabase Données	Base PostgreSQL, comptes et sessions, stockage des fichiers et des photos de terrain. Instance dédiée, provisionnée pour votre laboratoire seul.	France — région Paris	SOC 2 Type II · ISO 27001 Accord de sous-traitance art. 28
Sentry Supervision	Collecte des erreurs applicatives pour diagnostic. Aucune donnée personnelle transmise — le détail figure page 4.	Union européenne — Allemagne	SOC 2 Type II Accord de sous-traitance art. 28

Aucun transfert hors Union européenne

Données au repos, sauvegardes et journaux techniques restent dans l'Union. Aucun traitement, aucune réplication, aucun accès de support depuis un pays tiers.

Aucune empreinte sur vos postes

Rien à installer, rien à mettre à jour, aucune extension de la surface d'attaque de vos terminaux. Vos politiques de navigateur et de gestion de flotte s'appliquent sans adaptation.

Chiffré en transit et au repos

TLS 1.3 sur les liaisons, AES-256 sur les disques et les sauvegardes, y compris pour les fichiers et les photos. Rotation des clés assurée par l'hébergeur.

Chaîne de sous-traitance. La liste complète est annexée au contrat. Toute évolution vous est notifiée avant sa mise en œuvre, conformément à l'article 28 du RGPD, avec un délai suffisant pour exercer votre droit d'objection.

CE QUE L'APPLICATION DEMANDE À VOTRE SYSTÈME D'INFORMATION

Postes de travail	Un navigateur à jour — Chrome, Edge, Firefox ou Safari. Aucune installation, aucun droit administrateur, aucune exception à déclarer dans votre antivirus.
Mobiles et tablettes	Le même navigateur. L'application peut être épinglée à l'écran d'accueil, sans magasin d'applications ni distribution gérée.
Réseau	Un accès HTTPS sortant vers le domaine de l'application. Aucun flux entrant, aucun port à ouvrir, aucune adresse à publier depuis votre réseau.
Annuaire et messagerie	Aucun prérequis. L'authentification unique reste optionnelle ; les notifications passent par le navigateur, sans relais de messagerie ni enregistrement DNS à créer chez vous.

Authentification et contrôle d'accès

Chaque requête est authentifiée, et le rôle qui l'accompagne est revérifié côté serveur — jamais sur la seule foi de ce que déclare le navigateur.

LE PARCOURS D'UNE CONNEXION

01 — Identifiant
L'agent saisit son identifiant interne et son mot de passe. Aucune adresse électronique personnelle n'est demandée.

02 — Résolution
L'identifiant est résolu en compte technique par une fonction exécutée dans la base, jamais côté navigateur.

03 — Vérification
Comparaison à une empreinte bcrypt salée. Aucun mot de passe n'est lisible, pas même par l'administrateur.

04 — Session
Jeton signé à durée de vie courte, renouvelé par un jeton de rafraîchissement révocable à tout instant.

05 — Autorisation
Rôle et modules revérifiés côté serveur à chaque requête, puis une seconde fois par la base elle-même.

LES GARDE-FOUS

MOT DE PASSE
12 caractères
Longueur minimale imposée à la création du compte comme à chaque réinitialisation.

ANTI-FORCE BRUTE
5 essais
Puis blocage de 15 minutes par adresse, sur le formulaire de connexion.

CRÉATION DE COMPTE
Par l'administrateur
Pas d'auto-inscription, pas de réinitialisation en libre-service, pas de lien par courriel.

RÉVOCATION
Immédiate
Désactivation du compte et invalidation de la session, sans délai de propagation.

SUPPRESSION
Sans perte de trace
L'accès est coupé et le compte horodaté ; le nom reste lisible dans les archives réglementaires.

JOURNALISATION
Actions sensibles
Création de compte, changement de rôle, export, suppression : qui, quoi, quand.

LES PROFILS ET LEUR PÉRIMÈTRE

PROFIL	CE QU'IL CONSULTE	CE QU'IL ÉCRIT
Préleveur	Ses tournées, ses points, sa saisie du jour	Prélèvements, essais, signalements, photos
Encadrant prélèvement	L'activité terrain et son équipe	Planning, validation des tournées, référentiels terrain
Analyste	Demandes d'analyse et résultats	Résultats, prise en charge des demandes
Encadrant analyse	Le pôle analyse et son équipe	Arbitrage des demandes, planning du pôle
Logistique	Magasin, stock, commandes, réception	Mouvements de stock, réception d'échantillons
Encadrant logistique	Le pôle logistique et son équipe	Commandes, référentiel magasin, planning du pôle
Coordinateur	Vue transverse sur les trois pôles	Planning, annonces, arbitrages
Responsable de laboratoire	L'ensemble de l'activité	Tout, hors administration technique
Administrateur	Comptes, modules, paramètres, journaux	Administration complète
Exploitant — partenaire externe	Ses sondes, leurs étalonnages, ses demandes	Demandes de calibration et d'analyse, soumises à validation

Dix profils, trente-six modules. L'accès se règle par pôle métier, par module, et si nécessaire utilisateur par utilisateur. Un module désactivé n'est pas seulement masqué : l'écran, la route serveur et la base le refusent indépendamment.

Sécurité des données

La règle d'accès vit dans la base de données, pas seulement dans le code. Un défaut applicatif ne suffit donc pas à faire sortir une donnée de son périmètre.

DÉFENSE EN PROFONDEUR — QUATRE COUCHES INDÉPENDANTES

01
Base de données
Row Level Security
La politique s'applique à la requête elle-même, quel que soit le code qui l'émet. C'est la seule couche qui reste debout si toutes les autres tombent.

02
Action serveur
Identité revérifiée
Chaque écriture recharge l'utilisateur et son rôle depuis la session serveur avant d'agir. Rien n'est accepté sur déclaration du client.

03
Module
Route et export
Un contrôle d'appartenance au module précède l'accès à chaque page et à chaque export de fichier.

04
Interface
Confort, pas sécurité
Ce que l'utilisateur ne peut pas faire ne lui est pas proposé — mais cette couche n'est jamais comptée comme une protection.

CE QUI EST EN PLACE, EN CHIFFRES

TABLES	AVEC RLS ACTIVE	POLITIQUES D'ACCÈS	PROFILS DISTINCTS	SECRETS VERSIONNÉS
40	40	129	10	0

Relevé sur l'environnement de référence. Une table du registre éditeur porte volontairement zéro politique et aucun droit pour les rôles applicatifs : elle n'est accessible qu'au compte de service, et reste invisible même pour un administrateur authentifié.

TRANSPORT ET EN-TÊTES DE SÉCURITÉ

EN-TÊTE	EFFET
Strict-Transport-Security	Deux ans, sous-domaines inclus, préchargement — le navigateur refuse par avance toute liaison non chiffrée
Content-Security-Policy	Sources restreintes au domaine ; images et connexions sortantes limitées aux hôtes déclarés
X-Frame-Options	**DENY** — l'application ne peut pas être encadrée par un site tiers
X-Content-Type-Options	**nosniff** — le navigateur ne réinterprète pas le type déclaré d'une ressource
Referrer-Policy	Origine seule vers l'extérieur — aucune URL interne ne fuit vers un site tiers
Permissions-Policy	Caméra, microphone et géolocalisation désactivés au niveau du navigateur

TROIS SCÉNARIOS, TROIS RÉPONSES

Un défaut dans le code applicatif
La requête part quand même, mais elle part avec l'identité de celui qui l'a déclenchée. La politique de la base la filtre avant de répondre : au pire l'écran est vide ou en erreur ; il ne montre pas les données d'un autre périmètre.

Un jeton de session dérobé
Le jeton porte une identité, pas des droits : ceux-ci sont réévalués à chaque requête, côté serveur puis côté base. Sa durée de vie est courte, et la désactivation du compte l'invalide sans attendre son expiration.

Un compte interne compromis
L'attaquant hérite du périmètre de ce rôle, et de rien d'autre : un compte de préleveur ne devient pas administrateur. Les actions sensibles sont journalisées, et la révocation coupe l'accès sans délai de propagation.

Déploiement, continuité et supervision

Les mises à jour n'interrompent pas le service et se reprennent en une opération. La supervision est en place avant que l'utilisateur n'ait à signaler quoi que ce soit.

LE CHEMIN D'UNE MISE À JOUR

01 — Développement
Branche dédiée, base de développement distincte, jamais de donnée réelle.

02 — Contrôles
Compilation, typage et tests automatisés à chaque envoi ; un échec bloque la suite.

03 — Préproduction
Adresse de recette isolée, alimentée en données fictives, ouverte à votre validation.

04 — Validation
Promotion décidée explicitement. Aucune bascule automatique vers la production.

05 — Production
Bascule sans coupure de session, version précédente réactivable en une opération.

CONTINUITÉ DE SERVICE

DISPONIBILITÉ
99,5 %
Mesurée mensuellement, hors fenêtres de maintenance planifiées et annoncées 5 jours à l'avance.

SAUVEGARDES
Quotidiennes
Rétention 30 jours, chiffrées, conservées hors de l'instance de production.

RESTAURATION
Testée
Test de restauration semestriel, documenté et transmis. Une sauvegarde non restaurée n'est pas une sauvegarde.

RETOUR ARRIÈRE
Immédiat
Réactivation de la version précédente sans intervention sur les serveurs.

MAINTENANCE
Sans coupure
Les sessions ouvertes ne sont pas interrompues pendant un déploiement.

ENVIRONNEMENTS
Deux, séparés
Production et développement : bases, secrets et déploiements distincts, sans passerelle.

SUPERVISION ET JOURNAUX

- **Erreurs applicatives** — Chaque anomalie est capturée avec sa pile d'appel et regroupée par cause. **Aucune donnée personnelle n'est transmise** : ni nom, ni adresse, ni identifiant de connexion — seulement un identifiant technique et le rôle, pour situer l'incident.
- **Journaux d'accès** — Connexions, échecs répétés, actions d'administration et exports sont journalisés et consultables depuis l'application, sans passer par l'éditeur.
- **Vers votre SIEM** — Les journaux sont exportables au format standard vers Sentinel, Splunk ou équivalent. Le connecteur et sa fréquence sont chiffrés séparément.

Incident de sécurité. En cas d'accès non autorisé ou de suspicion de fuite, votre référent est notifié sans délai, avec les éléments nécessaires à votre propre notification à la CNIL dans les 72 heures. Les seuils d'alerte et les contacts d'escalade sont arrêtés conjointement à la mise en service.

ENGAGEMENT DE SUPPORT

SUPPORT
5j/7 · 9h – 17h
Par courriel et par téléphone. Interlocuteur unique, sans plateforme de premier niveau ni file d'attente.

PRISE EN COMPTE
4 h ouvrées
Accusé de réception qualifié : niveau de gravité attribué et suite donnée annoncée.

ANOMALIE BLOQUANTE
1 jour ouvré
Contournement ou correction. Est bloquante toute anomalie qui empêche une tournée ou une réception d'échantillons.

Protection des données personnelles

Votre laboratoire reste responsable de traitement ; l'éditeur intervient comme sous-traitant au sens de l'article 28. Le registre des traitements et l'analyse d'impact sont tenus à votre disposition.

CE QUI EST TRAITÉ

CATÉGORIE	DONNÉES	PERSONNES CONCERNÉES
Identité professionnelle	Nom, prénom, identifiant interne, rôle, équipe, type de contrat	Agents du laboratoire
Activité	Prélèvements, saisies, validations, horodatage des actions	Agents du laboratoire
Photos de terrain	Clichés rattachés à un point de prélèvement ou à une anomalie	Agents du laboratoire
Partenaires	Identité professionnelle et demandes des exploitants d'équipements	Partenaires externes
Journaux techniques	Identifiant technique, rôle, horodatage ; adresse réseau sur le seul formulaire de connexion	Tous les comptes

Ce qui n'est pas collecté. Aucune adresse électronique personnelle, aucun numéro de téléphone, aucune donnée sensible au sens de l'article 9, aucune géolocalisation des personnes. Les comptes sont créés par votre administrateur à partir d'un identifiant interne, et l'adresse technique du compte en est dérivée : elle ne correspond à aucune boîte réelle. La géolocalisation est refusée au niveau du navigateur, par en-tête.

DURÉES DE CONSERVATION

Comptes actifs	Durée de présence de l'agent dans l'organisation.
Comptes supprimés	Accès coupé immédiatement. Le nom reste lisible dans les archives, pour que la traçabilité réglementaire d'un prélèvement ne devienne pas anonyme après un départ.
Données opérationnelles	Durée fixée au contrat, alignée sur vos propres obligations de conservation.
Journaux d'audit	12 mois glissants, conformément à la recommandation de la CNIL.
Sauvegardes	30 jours glissants, chiffrées, purge automatique au-delà.
Fin de contrat	Restitution complète sous 15 jours en formats ouverts, puis suppression définitive de l'instance et des sauvegardes.

DROITS DES PERSONNES

Accès et rectification
Chaque agent consulte ses données depuis son profil. La rectification est faite par l'administrateur du laboratoire, sans intervention de l'éditeur.

Effacement
La suppression coupe l'accès sans délai. Ce qui subsiste est strictement ce qu'impose la traçabilité réglementaire des mesures, et rien d'autre.

Portabilité
Export libre-service et permanent, en formats ouverts, sans demande préalable ni facturation à l'acte.

SOUS-TRAITANCE ET RESPONSABILITÉS

Responsable de traitement	Votre laboratoire. Il détermine les finalités, les durées et les destinataires.
Sous-traitant	KSociety, enseigne de Karim Sehil, entrepreneur individuel — SIREN 944 922 780, immatriculée au Registre National des Entreprises.
Cadre contractuel	Accord de sous-traitance conforme à l'article 28, annexé au contrat de licence et signé avec lui.
Sous-traitants ultérieurs	Chaîne nommée au contrat. Toute évolution est notifiée avant mise en œuvre, avec un droit d'objection.
Registre et analyse d'impact	Tenus à jour et transmis sur demande, avec la documentation des mesures techniques de l'article 32.
Contact	karim.sehil@aquarys.io — 07 67 90 65 40

Intégration à votre environnement

L'application n'emploie que des standards du web. Les briques Microsoft que vous exploitez déjà s'y appliquent sans développement spécifique de votre côté.

MICROSOFT 365 ET ENTRA ID

Authentification unique

Connexion avec le compte Microsoft existant via OAuth 2.0 ou SAML 2.0. Désactiver le compte dans l'annuaire révoque l'accès à l'application, et l'attribution des rôles peut être pilotée depuis vos groupes.

Accès conditionnel et MFA

Double authentification, restriction aux postes conformes, blocage géographique : ces politiques s'appliquent côté Microsoft, sans modification de l'application.

Accès réseau restreint

L'application peut être rendue inaccessible depuis l'internet public et publiée derrière votre proxy applicatif ou votre VPN, pour les seuls postes gérés.

ÉTAT DES DISPOSITIFS

DISPOSITIF	ÉTAT
Chiffrement en transit et au repos	EN PLACE
Cloisonnement par rôle dans la base de données	EN PLACE
Environnements production et développement séparés	EN PLACE
Journal d'audit des actions sensibles	EN PLACE
Limitation des tentatives de connexion	EN PLACE
Instance dédiée, région Paris	À LA MISE EN SERVICE
Sauvegardes 30 jours et test de restauration semestriel	À LA MISE EN SERVICE
Authentification unique Entra ID et double authentification	SUR DEVIS
Export des journaux vers votre SIEM	SUR DEVIS
Publication derrière proxy applicatif ou VPN	SUR DEVIS
Hébergement souverain qualifié (SecNumCloud, HDS)	SUR DEVIS

En place — vérifié sur la version courante du produit. · **À la mise en service** — provisionné et engagé au contrat pour votre instance. · **Sur devis** — réalisable, chiffré séparément selon votre configuration.

CE QU'IL FAUT RETENIR

- **Rien à installer, rien à ouvrir**
  Aucun agent sur vos postes, aucun flux entrant vers votre réseau, aucune exception à créer dans vos politiques de sécurité.
- **Une instance par client**
  Pas de base partagée entre laboratoires. Le cloisonnement est une propriété de l'hébergement, pas une règle applicative qu'un défaut pourrait contourner.
- **Vous pouvez partir**
  Export permanent en formats ouverts, restitution sous 15 jours, aucun frais de sortie, dépôt du code source chez un tiers de confiance.

Audit technique, test d'intrusion ou revue d'architecture : à votre convenance.
Environnement de démonstration ouvert à votre DSI · aquarys.io/demo · karim.sehil@aquarys.io

Planifier la revue