Mesures techniques et organisationnelles

Accès, stockage, sauvegarde et gestion des incidents.

Information | Français | Version 1.0 | 30 octobre 2026

Accès et séparation

L'application utilise des comptes individuels et une authentification Better Auth. Les contrôles d'accès sont appliqués selon les utilisateurs, projets et organisations. Le stockage média principal a été vérifié privé le 6 octobre 2026. Le code contient un mécanisme d'URL signée avec une validité par défaut de cinq minutes ; une URL partagée reste utilisable par son détenteur pendant sa validité. Cela ne constitue pas une garantie que chaque parcours utilise la même durée. Les avatars facultatifs sont distincts des médias de projet : ils sont servis par des URL publiques Vercel Blob ; privilégier une image neutre. Une authentification multifacteur imposée à tous les utilisateurs, SAML et SCIM ne sont pas attestés dans le périmètre standard.

Administration et confidentialité

La politique limite l'accès administratif aux besoins de service, assistance, diagnostic et prévention des abus. Les engagements de confidentialité du personnel, revues d'accès et authentification renforcée des comptes privilégiés doivent être documentés contractuellement. Leur déploiement exhaustif n'est pas attesté par cette fiche.

Transport et secrets

Le service public utilise HTTPS. Les clés des fournisseurs sont destinées au serveur ; elles ne doivent pas figurer dans les documents clients. Les garanties de chiffrement au repos et de gestion des clés propres à chaque fournisseur sont celles de ses conditions et configurations vérifiées ; aucune gestion de clés dédiée au client n'est annoncée.

Sauvegarde et continuité

Le registre constate des sauvegardes quotidiennes de la base Supabase et une fenêtre standard de restauration de sept jours pour le forfait observé. Les objets Storage ne sont pas inclus dans ces sauvegardes de base. Une sauvegarde séparée chiffrée et un test de restauration isolé sont documentés en août 2026. Cela ne prouve ni un cycle automatisé complet des médias, ni un RPO/RTO contractuel. Le cycle des copies supplémentaires et leur effacement restent à formaliser.

Fournisseurs et changement

Le code contient une validation explicite des fournisseurs pour la production. La présence de ce contrôle ne prouve pas les valeurs effectivement déployées ni la signature de chaque DPA. Les justificatifs contractuels et le périmètre de chaque fonction doivent être validés avant une utilisation impliquant des données personnelles.

Incident

Signaler un incident à info@renderz.ch avec un objet « Incident de sécurité Renderz », la date, le service concerné et une description sans données sensibles. Renderz doit informer le responsable du traitement dans les meilleurs délais lorsqu'une violation affecte ses données et lui fournir les éléments nécessaires à son évaluation. Le responsable détermine ses obligations de notification à l'autorité et aux personnes ; aucun délai contractuel de 24 h ni assistance 24/7 n'est attesté ici.

Vérification fournisseur

Les preuves complémentaires, questionnaires et audits sont à convenir avec Renderz sous confidentialité si nécessaire. Aucun test d'intrusion indépendant récent, certification de Renderz ou disponibilité garantie n'est affirmé dans ce dossier.