Aperçu des mesures de sécurité

Version 1.0 | Dernière mise à jour : 29 septembre 2026

Cette page résume, pour un client ou son équipe de sécurité, les mesures techniques et organisationnelles en vigueur pour les services d'Avanserv SRL à la date figurant en tête de page. Elle complète, sans le remplacer, l'annexe B de l' accord de sous-traitance de données, qui a valeur contractuelle pour un client donné. Ce qui est planifié est présenté comme tel.

Hébergement

Les services sont hébergés par Scaleway SAS, société de droit français, dans la région fr-par (France). Le site et l'application sont servis depuis cette région. Un transfert hors de l'Union reste possible pour certains échanges avec des tiers, encadré comme le décrit l'article 9 de l'accord de sous-traitance de données pour un client, et la politique de confidentialité pour un visiteur du site.

Chiffrement

Les échanges avec le site et l'application sont chiffrés en TLS, le certificat étant émis et renouvelé automatiquement. La base de données de la plateforme app.avanserv.com est chiffrée au repos. Les cookies de session "access_token" et "refresh_token" sont marqués Secure et HttpOnly hors développement ; le cookie "avanserv_signed_in", qui indique au site public qu'une session existe ailleurs sans en révéler le contenu, est volontairement lisible par du code exécuté dans le navigateur et n'est pas marqué HttpOnly.

Séparation des organisations

La séparation entre organisations clientes est logique, sur une infrastructure partagée. Seuls les projets et les configurations d'authentification unique (SSO) d'une organisation sont filtrés par organisation à chaque lecture, écriture ou suppression, sans mécanisme pour le contourner depuis l'interface ou l'API. Les autres enregistrements, tels que les comptes, les fichiers et les réponses aux formulaires publics, ne sont pas soumis à ce filtre : les comptes rejoignent une organisation par une

adhésion plutôt que par ce filtre, et l'ensemble est protégé par le contrôle d'accès décrit ci-dessous.

Authentification et mots de passe

Les mots de passe ne sont jamais stockés en clair : seule une empreinte bcrypt est conservée. À la création ou au changement d'un mot de passe, une longueur minimale de 12 caractères est exigée et les mots de passe les plus courants sont refusés ; aucune règle de composition (majuscule, chiffre, caractère spécial) n'est imposée par défaut. Lorsque le service répond dans les trois secondes, le mot de passe est en outre vérifié contre les fuites connues auprès du service Have I Been Pwned, par comparaison d'un fragment d'empreinte cryptographique qui ne permet ni de reconstituer le mot de passe ni d'identifier une personne ; passé ce délai, la vérification est ignorée et le mot de passe est accepté.

Contrôle d'accès

Les droits sont attribués selon un modèle déclaratif fondé sur les rôles et les privilèges, appliqué à chaque requête : ce qui n'est pas explicitement autorisé est refusé.

Gestion des secrets

Les identifiants dont les services ont besoin en fonctionnement (mots de passe de base de données, clés applicatives) sont conservés dans le gestionnaire de secrets de Scaleway et synchronisés dans l'environnement d'exécution par un contrôleur dédié, à intervalle régulier (toutes les heures pour l'application) plutôt qu'au moment de chaque changement ; aucun secret n'est versionné dans le code.

Gestion des changements

Toute fusion de code vers la branche de production exige la réussite de l'intégration continue (formatage, analyse statique, typage, tests), sans exception. L'obligation de passer par une pull request en connaît une, réservée à une automatisation technique du dépôt. Les changements d'infrastructure passent eux aussi par une pull request, mais sont appliqués depuis le poste d'un opérateur plutôt qu'automatiquement à la fusion.

Sauvegardes

La base de données de la plateforme app.avanserv.com est sauvegardée une fois par jour, et chaque sauvegarde est conservée sept jours. Pour les données qu'un client héberge auprès du prestataire, la sauvegarde suit les conditions fixées au devis, comme le prévoient l'accord de sous-traitance de données et l'article 7 du SLA ; en l'absence de mention au devis, aucune sauvegarde n'est due.

Journalisation

Les requêtes servies par l'application sont journalisées avec un identifiant de requête ; une session ouverte y ajoute l'organisation et le compte concernés. Les adresses email sont masquées dans ces journaux avant leur écriture. Une collecte centralisée de ces journaux, de mesures et de traces, avec une alerte qui prévient une personne d'astreinte, est planifiée et n'est pas encore active : chaque journal reste aujourd'hui sur le nœud qui l'a produit, sous la rotation par défaut de l'environnement d'exécution.

Divulgation de vulnérabilités

Toute personne qui découvre une faille de sécurité dans nos systèmes peut nous la signaler selon la politique de divulgation coordonnée de vulnérabilités.

Notification en cas d'incident

Les engagements de notification en cas de violation de données à caractère personnel figurent dans l'accord de sous-traitance de données et dans la politique de confidentialité.

Pour toute question sur ces mesures : security@avanserv.com.