CHARTE — SÉCURITÉ

Charte de sécurité alan

Mesures techniques et organisationnelles de protection des données

Éditeur :	Version :	En vigueur :	RCCM :
afup SARL	1.0	07/06/2026	GA-LBV-01-2022-B12-00019

La présente charte décrit, à des fins d'information et de transparence, les mesures techniques et organisationnelles mises en œuvre par afup SARL pour protéger les données confiées par ses clients sur la plateforme alan. Elle complète les engagements contractuels figurant dans les CGV et le DPA.

1. Architecture cloisonnée par client

Chaque entreprise cliente dispose de son propre **schéma PostgreSQL dédié**. Cette isolation au niveau du système de gestion de base de données garantit qu'il est **techniquement impossible** qu'un client accède aux données d'un autre client. Le cloisonnement est imposé par l'infrastructure, pas seulement par le code applicatif.

2. Chiffrement des communications

Toutes les communications entre le navigateur de l'utilisateur et la plateforme sont chiffrées par **TLS 1.2 ou supérieur**. Les directives HSTS (HTTP Strict Transport Security) sont actives en production. Aucune communication ne peut donc être interceptée en clair, y compris lors d'une attaque par interposition.

3. Authentification renforcée

- Mots de passe d'au moins **douze (12) caractères**, avec exigence de minuscule, majuscule, chiffre et caractère spécial.
- Algorithme de hachage **Argon2id**, aujourd'hui recommandé pour le stockage des mots de passe.
- **Authentification à deux facteurs (2FA)** obligatoire pour les comptes administrateurs, gestionnaires de paie et membres de cabinet.
- Limitation des tentatives de connexion : 5 échecs / 15 min → blocage temporaire de l'adresse IP.
- Verrouillage automatique des comptes après 10 échecs / 24 heures, déblocage par un administrateur afup.

4. Défense en profondeur

- En-têtes HTTP renforcés : Content-Security-Policy, Permissions-Policy (caméra, micro, géolocalisation, paiement, USB bloqués au niveau du navigateur), X-Frame-Options DENY, Cross-Origin-Opener-Policy same-origin.

- Cookies HttpOnly + SameSite=Strict : impossibles à voler par script malveillant ou attaque CSRF.
- Pages authentifiées en Cache-Control: no-store : aucun proxy ou CDN ne peut conserver une copie.
- Validation systématique des entrées utilisateur.

5. Journalisation et auditabilité

Toutes les actions sensibles (connexions, modifications de salaires, validations de bulletins, déblocages de comptes, exports de données…) sont enregistrées dans un journal d'audit horodaté conservé pendant **douze (12) mois**. Ce journal permet d'identifier l'auteur, la nature et le moment exact de chaque action en cas d'incident.

6. Sauvegardes chiffrées et restauration testée

- Sauvegardes quotidiennes chiffrées par algorithme **Fernet (AES-128 CBC + HMAC-SHA256)**.
- Conservation 30 jours, purge automatique au-delà.
- Vérification d'intégrité par empreintes SHA-256.
- Procédure de restauration documentée et testée trimestriellement.
- Chiffrement effectué **avant** écriture sur le stockage de sauvegarde : l'accès au stockage seul ne donne pas accès aux données.

7. Hébergement

La plateforme alan est hébergée par **Hostinger International Ltd.** (61 Lordou Vironos Street, 6023 Larnaca, Chypre), opérateur lié par des garanties contractuelles de sécurité et de disponibilité.

8. Mises à jour de sécurité

Les composants applicatifs (Django, PostgreSQL, dépendances tierces) font l'objet d'une veille continue. Les correctifs de sécurité sont appliqués selon une politique de priorisation : correctifs critiques sous 48 heures, correctifs importants sous 14 jours.

9. Politique de divulgation responsable

Toute personne découvrant une vulnérabilité de sécurité est invitée à la signaler de manière confidentielle à **securite@afup-tech.com**. afup s'engage à accuser réception sous 72 heures et à ne pas engager de poursuites à l'égard des chercheurs en sécurité agissant de bonne foi.

10. Conformité loi 001/2011

Les mesures décrites ci-dessus répondent à la loi gabonaise n° 001/2011 sur la protection des données à caractère personnel, ainsi qu'aux bonnes pratiques internationales de sécurité de l'information. afup fait l'objet d'une déclaration auprès de la **Commission Nationale pour la Protection des Données à Caractère Personnel (CNPDCP)**.

11. Contacts sécurité

Sujet	Contact
Signalement de vulnérabilité	securite@afup-tech.com
Délégué à la protection des données	contact@afup-tech.com
Support général	support@afup-tech.com
Téléphone	+241 77 16 64 84

Mise à jour. La présente charte est revue annuellement et mise à jour à chaque évolution significative de l'architecture ou des mesures de sécurité. La version courante est toujours disponible sur https://alan.afup-tech.com/securite/.