

Sécurité de la Plateforme

Version: 1.0

Date d'entrée en vigueur: 25 septembre 2026

Dernière mise à jour: 25 septembre 2026

Langue faisant foi: Français / French / Frans

Version faisant foi. En cas de divergence entre les versions linguistiques, la version française prévaut, sous réserve des règles impératives applicables.

SPEC CONSTRUCTION TECHNOLOGIE SRL

Chaussée de Roodebeek 206, 1200 Woluwe-Saint-Lambert, Belgique

Entreprise / Ondernemingsnummer / Enterprise No.: 0844.731.626

TVA / BTW / VAT: BE 0844.731.626

E-mail: sct@sctwebcare360.com

Web: sctwebcare360.com

Sommaire / Inhoud / Contents

1. 1. Principes
2. 2. Comptes et authentification
3. 3. Autorisation
4. 4. Paiements
5. 5. Images et vidéos
6. 6. Journaux, sauvegardes et incidents
7. 7. Signalement de sécurité

1. Principes

SCT WebCare 360 applique une défense en profondeur : contrôles d'accès côté serveur, moindre privilège, isolation des environnements, protection des secrets, validation des entrées, journalisation et sauvegardes.

2. Comptes et authentification

- Mots de passe hachés avec les mécanismes sécurisés disponibles en PHP.
- Sessions HttpOnly/Secure sous HTTPS avec paramètres SameSite adaptés et rotation d'identifiant.

- Authentification multifacteur/TOTP lorsque requise pour les rôles sensibles.
- Appareils de confiance limités dans le temps et révocables.
- Limitation des tentatives et journalisation des connexions suspectes.
- Changement de mot de passe, e-mail, rôle ou MFA pouvant invalider les anciennes sessions.

3. Autorisation

Les rôles et la propriété des ressources sont vérifiés au serveur à chaque requête. Une entreprise ne peut ni lire ni modifier les annonces, médias ou données privées d'une autre entreprise par simple changement d'identifiant.

4. Paiements

Les Checkout sont créés côté serveur à partir du catalogue de prix. Les webhooks Stripe sont signés et idempotents. Les clés sont conservées hors du code public et le mode test/live est vérifié. Les données complètes de carte ne sont pas stockées par la Plateforme.

5. Images et vidéos

Les uploads sont contrôlés par MIME/type réel, taille, propriété, limites de forfait et CSRF. Les vidéos sont traitées par un worker isolé avec FFmpeg, signatures HMAC, protections anti-replay et stockage privé/public séparé. Seuls les médias approuvés sont exposés publiquement.

6. Journaux, sauvegardes et incidents

Les événements d'audit et de sécurité sont conservés selon la Politique de confidentialité. Les sauvegardes sont conservées hors du webroot. En cas d'incident, l'Opérateur peut révoquer des sessions, bloquer des fonctions, préserver les preuves et effectuer les notifications légales requises.

7. Signalement de sécurité

Un problème de sécurité peut être signalé à sct@sctwebcare360.com. N'incluez pas de mots de passe, clés privées ni autres secrets dans un message non chiffré. L'Opérateur peut demander des informations techniques supplémentaires.