

Platform Security

Version: 1.0

Effective date: 25 September 2026

Last updated: 25 September 2026

Controlling language: Français / French / Frans

The French version is controlling. In case of any discrepancy between language versions, the French version prevails unless mandatory law provides otherwise.

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. Principles
2. Accounts and authentication
3. Authorisation
4. Payments
5. Images and videos
6. Logs, backups and incidents
7. Security reporting

1. Principles

SCT WebCare 360 uses defence-in-depth: server-side access control, least privilege, environment separation, secret protection, input validation, logging and backups.

2. Accounts and authentication

- Passwords hashed using secure PHP mechanisms.
- HttpOnly/Secure session cookies on HTTPS with appropriate SameSite settings and session ID rotation.
- MFA/TOTP for sensitive roles where required.

- Time-limited, revocable trusted devices.
- Rate limiting and logging of suspicious login attempts.
- Password, email, role or MFA changes may invalidate earlier sessions.

3. Authorisation

Roles and resource ownership are verified server-side on every request. One business cannot access or alter another business's private ads, media or data by changing an identifier.

4. Payments

Checkout sessions are created server-side from the pricing catalogue. Stripe webhooks are signed and idempotent. Keys are stored outside public code and test/live mode is checked. The Platform does not store full card details.

5. Images and videos

Uploads are validated by real type/MIME, size, ownership, CSRF and plan limits. Video processing uses an isolated FFmpeg worker, HMAC signatures, replay protection and separate private/public storage. Only approved media is served publicly.

6. Logs, backups and incidents

Audit/security events follow Privacy Policy retention. Backups are kept outside the webroot. During an incident, the Operator may revoke sessions, block functions, preserve evidence and make legally required notifications.

7. Security reporting

Security issues may be reported to sct@sctwebcare360.com. Do not send passwords, private keys or other secrets in an unencrypted message. The Operator may request additional technical information.