Information Security Policy

Version 1.0 — Effective 9 October 2026 · Reviewed annuallyApplies to: Zephir Solutions (Laura Gioia), all production systems and services operated for LauraSoap and partner projects.

1. Purpose and scope

This policy defines the security principles and mandatory practices for all information systems operated by Zephir Solutions. It covers self-hosted production servers, cloud services in use, administrative endpoints, and all customer and partner data handled on behalf of sellers, including TikTok Shop seller data.

2. Roles and responsibilities

- A single designated administrator (the company owner) is responsible for implementing and enforcing this policy.
- The policy is reviewed and re-approved at least once per year, and after any significant security incident.
- No third parties are granted administrative access to production systems.

3. Access control and least privilege

- All systems are accessed through dedicated, individually attributable accounts. Shared accounts are prohibited.
- Server administration uses SSH public-key authentication only; password authentication is disabled.
- Privileges follow least privilege: services run as unprivileged users inside isolated containers; the administrator uses elevated privileges only when required.
- All administrative and cloud accounts (source code hosting, email platform, DNS, app stores, partner portals) are protected with multi-factor authentication.
- Access to personal data is limited to what each service strictly requires to operate.

4. Security baseline for daily operations

- Endpoints in use for administration run a supported Linux operating system with automatic security updates enabled (unattended-upgrades).
- Unique, strong passphrases are stored in a password manager; credentials are never reused across services.
- Devices are screen-locked when unattended; disks and documents are kept in a private, access-controlled workspace.
- Only software required for business operations is installed.

5. Network security and segregation

- Every service runs in its own Docker container with a dedicated isolated Docker network; services can only reach the dependencies they are explicitly connected to.
- The only public entry points are HTTP/HTTPS through a hardened reverse proxy with TLS 1.2+ (Let's Encrypt certificates, automatic renewal).
- Databases and internal services listen on private interfaces only and are never exposed to the Internet.
- Remote administration happens exclusively over an encrypted WireGuard-based mesh VPN; management ports are not exposed to the public Internet beyond SSH.
- Brute-force and intrusion prevention on the SSH service is enforced with fail2ban.

6. Data classification and encryption

• All data in transit is encrypted: public endpoints over HTTPS/TLS 1.2+, inter-host traffic over the encrypted mesh VPN.

• Secrets (API keys, tokens, database credentials) are stored in environment files with owner-only permissions (0600), are excluded from version control, and are never embedded in public pages or repositories.

• Customer and seller data is processed following data-minimisation: only the fields required by the subscribed TikTok Shop event types are stored.

7. Vulnerability and threat management

• Operating-system security patches are applied automatically (unattended-upgrades); container base images are rebuilt and redeployed when updates are published.

• Public-facing services run behind the reverse proxy with the minimum set of open ports (80/443; SSH key-only on a non-standard administrative port).

• Repeated failed authentication attempts are blocked automatically by fail2ban.

8. Incident response and breach notification

• On suspected incident: contain (stop or isolate the affected service), rotate all potentially exposed credentials, assess the data and systems impacted.

• Where personal data is affected, the competent supervisory authority (CNIL, France) and affected data subjects are notified within 72 hours as required by GDPR.

• Sellers and platform partners (including TikTok Shop) are notified without undue delay through the contact channel registered with the partnership.

• A short post-incident review documents root cause and corrective actions.

9. Endpoint protection statement

All company endpoints used for administration run hardened, supported Linux systems with automatic security patching; the fleet contains no Windows endpoints without anti-virus protection. Server attack surface is minimised as described in section 5, and integrity of deployed code is ensured through private, access-controlled version control with signed commits audit trail.

Contact — For any security question or incident report: info@zephir.solutions

Zephir Solutions · France · zephir.solutions