

SCALEON ERP

Information Security & Data Protection Program

Field	Value
Organization	SCALEON ERP (scaleonerp.com.br) — multi-tenant SaaS ERP for e-commerce sellers
Legal entity	59.770.797 NICOLAS GOMES LIMA — CNPJ 59.770.797/0001-59 (Brazil)
Document version	1.2
Effective date	October 14, 2026
Review cadence	At least annually, and after any security incident or material system change
Owner / approver	Gabriel Molina Teramoto — Founder, Security & Privacy Owner
Privacy / DPO contact	privacidade@scaleonerp.com.br
Scope	All SCALEON systems, staff and contractors that access, process, store or transmit seller, buyer or TikTok Shop data
Related documents	Personal Information Protection Standard (SCL-PIPS-001)

Contents: 1. Information Security Policy · 2. Network Security · 3. Endpoint Protection · 4. Security Baseline · 5. Access Control Policy · 6. Data Classification & Encryption · 7. Incident Response Policy · 8. Vulnerability Management · 9. Internal Personal Data Protection Policy (LGPD) · 10. Data Subject Requests, Retention & Deletion · 11. Breach Notification · Annex A — Data inventory & sub-processors

1. Information Security Policy

SCALEON is a small SaaS company. Security responsibilities are formally assigned and this program applies to every person and system that handles customer data. The Founder is accountable for the program, approves this document and reviews it at least annually.

Role	Responsibilities
Security & Privacy Owner (Founder)	Approves policies; grants/revokes access; owns incident response and breach notification; LGPD data protection contact (encarregado).
Lead Developer	Implements technical controls (encryption, secrets, network rules, logging); applies patches and dependency fixes; first responder for technical incidents.
All staff / contractors	Follow this program; use MFA; report suspected incidents immediately; access data only for assigned tasks.

Principles: data minimization (only the TikTok Shop API scopes required for order, product, inventory and fulfillment management are requested), least privilege, encryption by default, use of reputable managed cloud providers, and documented response to incidents.

2. Network Security & Segregation

- SCALEON runs entirely on managed cloud infrastructure; there is no on-premises server or office network holding customer data.

- Application hosting: Vercel (serverless functions). Only HTTPS (TLS 1.2+) is exposed; HTTP is redirected to HTTPS. Vercel provides platform-level DDoS mitigation and firewall.
- Database: Neon managed PostgreSQL (region São Paulo, Brazil). Connections require TLS and credentials; the database is not exposed to anonymous access.
- File storage: Vercel Blob (labels, imported spreadsheets, photos, attachments, backups); access only from the application via server-side tokens.
- Environment segregation: Production, Preview and Development environments are separated, each with its own environment variables/secrets; development uses separate database branches and never production customer data.
- Monitoring: platform logs and alerts from Vercel and Neon are reviewed by the Lead Developer; anomalies (error spikes, unusual traffic, failed logins) trigger the incident process (Section 7).
- TikTok Shop API credentials (app secret, access/refresh tokens) are stored only as encrypted server-side secrets and never exposed to the browser.

3. Endpoint Protection

- All company computers used to access SCALEON systems run an up-to-date operating system with built-in anti-malware enabled (Microsoft Defender Antivirus with real-time protection and automatic definition updates, or the OS-equivalent).
- Automatic OS and browser updates are enabled; full disk encryption (BitLocker / FileVault) is enabled where supported.
- Servers/cloud workloads are managed by the providers (Vercel, Neon), which maintain host-level protection and patching.
- Devices are checked at least quarterly to confirm protection is active and up to date.

4. Security Baseline for Daily Operations

- Multi-factor authentication (MFA) is mandatory on all administrative/infrastructure accounts used by staff: Vercel, Neon, GitHub, e-mail and TikTok Shop Partner Center. (End-user login to the application currently uses e-mail and password; MFA for end users is on the roadmap.)
- Strong unique passwords (minimum 12 characters) stored in a password manager; no shared accounts; no credentials in source code.
- Automatic screen lock after at most 5 minutes of inactivity; devices are locked when unattended (clean desk / clear screen).
- Customer data is not exported to personal devices or spreadsheets except when strictly needed for a task, and such files are deleted afterwards.
- Staff and contractors receive security awareness guidance on onboarding and at least annually (phishing, MFA, data handling).

5. Access Control Policy

- Access follows need-to-know and least-privilege. Only the Founder and the Lead Developer have production access; any new access is requested and approved by the Founder.
- Application-level role-based access control (RBAC) and multi-tenant isolation: every record is scoped by tenant (seller) ID, and a seller can access only its own shops and data.
- Each person uses an individual named account; administrative actions are logged by the cloud providers.

- Access is reviewed at least every 6 months, and revoked within 24 hours when someone leaves or changes role (accounts disabled, tokens and secrets rotated).
- Seller authorization to TikTok Shop is via OAuth; sellers can revoke authorization at any time in TikTok Shop, after which the stored tokens stop working and are deleted on request.

6. Data Classification & Encryption

Class	Examples	Handling
Confidential — Personal	Buyer name, shipping address, phone, order details received from TikTok Shop	Encrypted in transit and at rest; least-privilege access; retained only while needed for fulfillment
Confidential — Secrets	App secret, OAuth access/refresh tokens, DB credentials, API keys	Stored only as encrypted environment secrets; never logged; rotated on suspicion of exposure
Internal	Products, SKUs, inventory, production orders, financial summaries	Access limited to the seller tenant and authorized staff
Public	Marketing site content	No restrictions

- **In transit:** TLS 1.2 or higher for all traffic (browser-to-app, app-to-database, app-to-TikTok Shop API, app-to-storage and to sub-processors).
- **At rest:** integration credentials (TikTok Shop access/refresh tokens) are encrypted by the application with AES-256-GCM; the Neon database, Vercel Blob files and Vercel environment secrets rely on the providers' managed encryption at rest.
- Keys are managed by the cloud providers' key management systems; no RSA-1024 or weaker algorithms are used.

7. Incident Response Policy

Step	Action	Owner / timing
1. Report	Anyone who suspects an incident reports immediately to the Security Owner (e-mail privacidade@scaleonerp.com.br / phone / WhatsApp).	All staff — immediately
2. Triage	Assess severity (data exposed? which tenants? ongoing?) and open an incident record.	Security Owner + Lead Dev — within 4 h
3. Contain	Revoke/rotate affected credentials and tokens, block access, disable affected features, preserve logs.	Lead Dev — immediately after triage
4. Notify	If personal data may be affected: notify TikTok Shop and affected sellers (Section 11) and, when required, the ANPD and data subjects under LGPD.	Security Owner — within 24 h to TikTok Shop / sellers
5. Recover	Fix root cause, restore from backup if needed, verify.	Lead Dev
6. Review	Post-incident review with root cause and preventive actions; update this program.	Security Owner — within 10 business days

An incident response tabletop exercise is performed at least annually and documented.

8. Vulnerability & Threat Management

- Source code is hosted on GitHub with automated dependency vulnerability alerts (Dependabot) and *npm audit*; critical/high findings are fixed within 7 days, medium within 30 days.
- Frameworks and libraries are kept on supported versions; security patches for the OS and browsers on company devices are applied automatically.
- Code changes are reviewed before deployment to production; secrets scanning is enabled on the repository.
- Fixes are tracked as issues in the repository until closed, retaining evidence of remediation.
- Cloud provider security advisories are monitored and applied.

9. Internal Personal Data Protection Policy (LGPD)

SCALEON acts as a data **processor (operador)** on behalf of sellers (controllers) for buyer data obtained through TikTok Shop, and complies with the Brazilian General Data Protection Law (Lei 13.709/2018 — LGPD) and the TikTok Shop Developer Terms.

- Collection: only data needed to provide order management, fulfillment, inventory and reporting features is collected, via authorized TikTok Shop API scopes; other marketplaces' data enters only through files exported and uploaded by the seller.
- Use: data is used solely to provide the service to the authorizing seller; never sold, used for advertising, or shared with other sellers.
- Storage: database in Brazil (Neon, São Paulo); application runtime and some files/processing in the United States (Vercel, Labelary, Resend, Inngest), protected as described in Sections 2–6.
- Sharing: only with the sub-processors listed in Annex A, under their data processing terms.
- Deletion: per Section 10.
- Maintenance: this policy is reviewed at least annually and whenever processing changes.

10. Data Subject Requests, Retention & Deletion

- Requests from sellers or TikTok Shop to provide, correct or delete user data are received at privacidade@scaleonerp.com.br or via the TikTok Shop partner channel, logged, verified and fulfilled within 15 days (or sooner if TikTok Shop or law requires).
- Automated retention already in place: shipping label PDFs deleted after 10 days; printed tracking-code records kept 30 days; database backups limited to the last 4 weekly + 1 monthly for 12 months.
- Other data is kept while the seller account is active or as required by law, and no longer than permitted by the TikTok Shop Developer Terms.
- When the contract ends, or upon request from the seller or TikTok Shop (including after de-authorization), the Security Owner runs the deletion procedure: TikTok Shop tokens are deleted immediately and all of that seller's marketplace data is permanently deleted from the database and file storage within 30 days; backups expire on the cycle above. Deletion is logged and confirmed to the requester.

11. Data Breach Notification

If a breach affecting TikTok Shop or seller data is suspected or confirmed, the Security Owner notifies TikTok Shop (via Partner Center support ticket and partner@tiktokshop.com) and affected sellers (via e-

mail) without undue delay and within 24 hours of confirmation, describing the nature of the incident, data and tenants involved, containment actions and contact point. Notifications to the ANPD and data subjects are made when required by LGPD.

Annex A — Data inventory & sub-processors

Sub-processor	Purpose	Data	Location
Vercel	Hosting / serverless runtime; logs	All application data in transit	United States (default region)
Vercel Blob	File storage and backups	Shipping labels (buyer name, address, phone), spreadsheets, photos, attachments, backups	Per Blob store region
Neon	Managed PostgreSQL database	All system data (orders, buyer shipping data, products, inventory)	Brazil (São Paulo)
Inngest	Background jobs	Job identifiers and metadata	United States
Resend	Transactional e-mail	Recipient name/e-mail, notice content	United States
Labelary	ZPL label rendering	Label content incl. buyer data	United States
Lalamove	Production freight	Workshop contact names, phones, addresses (not buyers)	Brazil
GitHub Actions	Runs weekly backup job	No stored data (backup saved to Vercel Blob)	United States
TikTok Shop Open API	Source of seller/order data	Orders, products, logistics	TikTok Shop

Data flow: Seller authorizes SCALEON via TikTok Shop OAuth → SCALEON backend (Vercel) calls the TikTok Shop API over TLS → data stored in Neon (São Paulo) and labels in Vercel Blob → displayed only to the authorizing seller's users → labels auto-deleted after 10 days; remaining data deleted at contract end or on request.

Approved by: Gabriel Molina Teramoto, Founder — October 14, 2026