Information Security & Privacy Policy

Operator	Lumiction Inc.
Service	Futari Sankyaku FC Portal
Headquarters	4-6-1-1314 Kachidoki, Chuo-ku, Tokyo, Japan
Responsible officer	Naoto Toda, Representative Director
Security / privacy contact	n-toda@lumiction.com
Public policy	https://23-fc-portal.com/legal/security/

1. Scope and accountability

This policy applies to company personnel, contractors and systems that operate the portal or handle seller, creator, maker, buyer or other personal data. The Representative Director is accountable for security, privacy, access approval, incident escalation and exceptions. Review this policy at least annually and after material service, legal or platform changes. Policies do not replace implementation verification.

2. Data minimization and classification

Collect only the data needed for the authorized service and granted API scopes. Restricted information includes credentials, OAuth tokens, bank information and password hashes. Confidential information includes order/customer data, support records and business records. Internal operational records are access restricted; only information intended for publication is Public. Do not use TikTok customer data for advertising or unauthorized purposes.

3. People and access governance

Grant access only to designated people for their work. Record the system, role, approver and access dates in the internal access register. Remove or review access on departure or role change and at least annually. Company endpoints must maintain anti-malware protection, updates, screen locking and protected accounts. Administrative services require MFA. The responsible officer confirmed coverage of all five company devices and principal services on 23 October 2026; this is an owner declaration, not an independent audit.

Access, encryption and service providers

4. Application and network protection

Use separate production and disposable test databases. The production application and managed PostgreSQL run as separate Render services in Singapore using an internal database connection. Remove unnecessary external database access. Serve public traffic over HTTPS, apply security headers and rate limiting, and monitor provider health and application security/error records. Do not claim a standalone NIDS/HIPS installation when relying on managed-provider and application controls.

5. Authentication and authorization

Separate franchisee, maker and headquarters access server-side and scope data to the authenticated tenant. Only the maker owner may request account erasure. Invalidate disabled staff sessions. Private uploaded files require authorization in addition to metadata access. Passwords use salted scrypt hashes; sessions use signed HttpOnly/Secure/SameSite cookies. Apply inactivity expiry, password-reset revocation and cross-site request checks. Production headquarters login requires a password plus an authenticator code; reject reused codes and invalidate old sessions when credentials change.

6. Encryption and secret handling

Use HTTPS for external transport. Render encrypts managed PostgreSQL, its backups, persistent disks and disk snapshots at rest. Additionally encrypt stored OAuth tokens and bank information with AES-256-GCM and separate secrets. Validate required production keys, restrict their access, and never put credentials, OTPs, raw customer payloads or full bank/card data into ordinary logs, exports or source control. Do not store payment card numbers or CVV. Only approved provider tokens and masked card metadata may be retained.

7. Locations and processors

Production application/database storage is in Singapore. Authorized company personnel operate from Japan. Resend processes/stores transactional email recipients, message content and delivery records in the United States; the sending region does not change the storage country. Minimize personal data in notifications. External AI inference is disabled until data categories, processing countries and provider terms have been separately assessed and approved. Optional object storage requires its own access, versioning and cache assessment; private images must not be exposed through a public bucket.

8. Vulnerability management

Record findings, severity, owner, remediation and verification. Run type checks, regression tests, isolated-database tests and dependency audits before release. Prioritize critical issues and restrict affected integrations when needed. Internal automated tests and remediation records do not constitute an independent penetration test, ISO certification or SOC report.

Protect the full data lifecycle

9. Rights requests and contract-end deletion

Receive seller, buyer and TikTok Shop requests through the privacy contact. Authenticated portal owners may use https://23-fc-portal.com/legal/data-request/ . Verify identity, authority and scope; normally respond within 30 days, explaining any delay. Do not ask for passwords, OTPs or card details by email. After headquarters approval, stop account access and credentials and erase associated personal/operational data. TikTok deauthorization starts erasure of TikTok data without cancelling the separate portal account.

10. Erasure execution and failure handling

Remove tokens, buyer names/addresses/telephone numbers, raw order/webhook payloads, external identifiers, retry queues and associated uploaded files. A durable pre-upload manifest preserves cleanup obligations after a crash. Reduce retained accounting to minimal pseudonymous amounts and internal references; document any separately required identifying legal records, basis, restricted access and expiry. Database ownership fences and SHA-256 erased-identifier records prevent delayed callbacks, notifications and sync jobs from re-creating data. Failures remain incomplete and are retried; they must never be represented as successful deletion.

11. Backups, copies and restoration

Record application-local erasure separately from full completion. Confirm processors, cached copies, object versions, exports and backup expiry before marking the request complete. Render point-in-time backups normally cover 3-7 days depending on workspace plan; logical exports are retained for 7 days. Resend standard email/log retention is 30 days. Inventory off-provider copies separately. Maintain a deletion ledger in approved encrypted storage separate from database backups. Before exposing a restored database, apply current migrations and reapply the latest ledger and erasure process. If verification fails, keep the restored system isolated.

12. Incident response and notification

Escalate suspected incidents immediately to Naoto Toda at n-toda@lumiction.com. Triage, contain, revoke or rotate affected credentials, assess affected data/tenants, preserve restricted evidence, remediate and verify recovery. Notify TikTok Shop through Partner Center support and affected sellers through registered contacts without undue delay and within applicable deadlines. The internal target is within 72 hours of confirmation, or sooner when required. Record notifications, open questions, follow-up and post-incident actions; review the response procedure and contacts at least annually.

References: TikTok DSPR requirements (partner.tiktokshop.com/docv2/page/data-security-and-privacy-review); Render PostgreSQL encryption, recovery and disk documentation (render.com/docs); Resend retention and storage disclosure (resend.com/security/gdpr). Public privacy notice: https://23-fc-portal.com/legal/privacy/ .