

ABI PILOT, LLC

Information Security Policy & Architecture Baseline

Official Partner Compliance Document | TikTok Shop Partner Security Review

Legal Entity: Abi Pilot, LLC

State of Formation: Delaware, USA

Primary Platform Domain: <https://abipilot.com>

Registered Address: 131 Continental Dr,
Suite 305, Newark, DE 19713

Effective Date: September 2026

Document Version: 1.0 (Enterprise)

Classification: External Compliance

Compliance Contact:
privacy@abipilot.com

1. Purpose, Scope & Commitment

This Information Security Policy defines the structural, operational, and organizational controls implemented by **Abi Pilot, LLC** ("AbiPilot") to safeguard tenant, seller, and platform data across all supported channels, with explicit application to the **TikTok Shop Partner Center (TTSPC)** API ecosystem. AbiPilot operates an enterprise multi-tenant software-as-a-service (SaaS) and autonomous orchestration platform, maintaining strict alignment with international confidentiality, integrity, and availability standards.

2. Cloud Infrastructure & Hosting Perimeter

- **Infrastructure Provider:** All production workloads, databases, and microservices are exclusively hosted within **Google Cloud Platform (GCP)** data centers located in the **United States**.
- **Physical & Environmental Security:** AbiPilot inherits physical facility controls, ISO/IEC 27001, SOC 1, SOC 2 Type II, and PCI-DSS compliance certified directly through Google Cloud's verified facilities.
- **Network Isolation & Perimeter Defense:** Systems operate inside dedicated Virtual Private Clouds (VPCs) with zero public accessibility to backend databases, enforced via strict Google Cloud Armor Web Application Firewall (WAF) rules and ingress/egress filtering.

3. Cryptographic Standards & Data Segregation

- **Encryption in Transit:** All API communications, administrative access, and webhook transmissions are strictly encrypted using **TLS 1.3** (with backward compatibility restricted to TLS 1.2 minimum). Unencrypted HTTP traffic is systematically rejected.
- **Encryption at Rest:** Persistent storage volumes, object stores, and database engines utilize **AES-256** symmetric encryption with automated key rotation managed by GCP Key Management Service (KMS).
- **Multi-Tenant Isolation:** Cross-tenant data mingling is cryptographically prevented at the application and query layers using strict, row-level `TenantId` partitioning. Each customer workspace is completely isolated.

4. Access Control, Identity & Secret Management

- **Least Privilege Principle (PoLP):** Access to administrative consoles and production clusters follows Role-Based Access Control (RBAC). Personnel receive only the minimal permissions

necessary for operational duties.

- **Multi-Factor Authentication (MFA):** Mandatory hardware or time-based one-time password (TOTP) 2FA is enforced across all engineering repositories, cloud IAM accounts, and operational consoles.
- **API Credential Protection:** TikTok Shop *App Key*, *App Secret*, and OAuth tokens are stored in tamper-evident secrets managers, transmitted exclusively in-memory, and strictly excluded from client-side bundles or persistent logs.

5. Endpoint Security & Operational Baselines

- **Endpoint Protection:** All administrative workstations accessing company infrastructure must execute modern Endpoint Detection and Response (EDR) / antivirus suites with automated signature updating.
- **Operational Policies:** Enforced screen locking after 5 minutes of inactivity, full-disk encryption (BitLocker / FileVault), and enterprise password complexity policies.

6. Privacy Compliance, Data Retention & DSAR

- **Regulatory Compliance:** AbiPilot adheres to GDPR, CCPA, and TikTok Commercial Data guidelines.
- **Data Subject Access Requests (DSAR):** We maintain dedicated automated endpoints to process real-time user data deletion, modification, and data retrieval requests initiated by TikTok Shop or merchants.
- **Contract Termination Purge:** Upon service termination or authorization revocation by a TikTok Shop seller, all associated synchronization caches are automatically purged within 30 days.

7. Incident Response, Vulnerability & Threat Management

- **Static & Dynamic Security Audits:** CI/CD pipelines run automated static analysis (SAST) and container image vulnerability scans prior to production deployment.
- **Security Incident Protocol:** A defined incident escalation protocol triages events 24/7. In the event of a verified breach impacting merchant or TikTok Shop data, notification will occur within 24 to 72 hours in compliance with applicable statutory timelines.
- **Breach History:** In the past three (3) years, Abi Pilot, LLC has experienced zero (0) data breaches, regulatory notices, or privacy complaints.

8. Corporate Attestation & Officer Sign-Off

I hereby certify that the security practices, encryption baselines, and data governance policies described herein accurately represent the operational architecture of Abi Pilot, LLC.

Authorized Representative:

Francisco Marcelino Muro Ampuero

Legal Entity: Abi Pilot, LLC

Date of Attestation: September 4, 2026

Verification Status: Active & Verified

Corporate Title:

Founder & Managing Member

Data Protection Contact:

privacy@abipilot.com

Jurisdiction: Delaware, USA

