Security and Privacy Policy Package

Version 1.0 · 13 November 2026 · Proposed; pending operator adoption

Purpose

Operational controls and proposed procedures for a single-operator, internal affiliate application. Prepared to support factual security/privacy assessment responses.

Current implementation

API secrets, KV values and authentication records use Windows DPAPI CurrentUser. The app now requires operator authentication for pages, APIs and media. Login rate limiting, session expiry, Origin/Host checks, audit events and controlled data-handling actions were added.

Adoption and scope

The owner must review this package, create the local operator password and record their name/date/acceptance in the Security screen before treating these procedures as adopted. This package does not appoint a DPO or assert ISO/SOC certification.

Important limits

Full-drive encryption, external account MFA, workstation auto-lock and network segmentation have not been verified. The entire SQLite database and media are not encrypted by the app. Data-processing countries for external providers remain to be mapped.

Evidence

Native DPAPI self-test and migration checks passed. The dependency audit was repeated after patching pip and reported no known vulnerabilities. Further implementation evidence and the operator’s adoption record are exported from the Security screen; do not attach a proposal as if it were already approved.

Information Security Policy

Version 1.0 · 13 November 2026 · Proposed; pending operator adoption

Purpose and scope

This policy covers the single-operator Afiliado Studio application, its local workstation, the Helios Soluções institutional website and authorized API connections. It is designed for the owner’s internal affiliate activity. It does not represent a certification or a TikTok approval.

Accountability and adoption

The application operator is responsible for access, backups, incident triage, requests and reviews. Version 1.0 is a proposal until the operator records their name, date and acceptance in the application. No DPO is appointed by this document. Contact: delevedoves@gmail.com.

Operational requirements

Use a dedicated, password-protected Windows account; do not share credentials. Lock the workstation when unattended, keep the workspace clear of exposed documents and credentials, and use MFA on external accounts wherever supported. These workstation and account controls require operator verification; the application does not configure them automatically.

Review and evidence

Review this package within 90 days of adoption and after material changes or an incident. Record adoption/review in the app. Run the technical controls check monthly and after security changes. Preserve dated results without including credentials. Missing controls remain open findings rather than being declared implemented.

Access Control and Least Privilege

Version 1.0 · 13 November 2026 · Proposed; pending operator adoption

Implemented access boundary

The app is intended to bind to 127.0.0.1. Pages, APIs and media require an authenticated local operator. Request Host and POST Origin are checked. Public OAuth callbacks are exceptional and must validate a one-time state with a 15-minute lifetime. This is a local application boundary, not a claim of enterprise network segmentation.

Operator authentication

The operator must create a 14-128 character passphrase. Passwords are hashed using PBKDF2-SHA256 with a random salt and 600,000 iterations. Five failed attempts in 15 minutes block further login attempts in that window. A new login replaces the previous session. Sessions expire after 15 minutes idle or eight hours total and can be revoked with the lock/logout control.

Roles and external permissions

There is one application operator and no multi-user role administration. Restrict each API integration to required scopes and review granted permissions after authorization. Do not share application credentials or export tokens. The app does not implement MFA; external account MFA and Windows access controls must be verified by the operator.

Offboarding

Stop scheduled activity, revoke authorizations through the relevant platform, remove local connections, follow the data deletion procedure, and confirm backups/exports are included. Changing an API key does not itself invalidate an already-issued OAuth token.

Data Classification, Handling and Protection

Version 1.0 · 13 November 2026 · Proposed; pending operator adoption

Classification

Public: institutional pages and approved product marketing information. Internal: generated scripts, videos, queue metadata and operational notes. Confidential: order/commission cache and privacy/incident case details. Restricted: API secrets, OAuth tokens, authentication records and recovery snapshots.

Implemented protection at rest

API secrets are stored in a DPAPI CurrentUser vault. All KV values, including OAuth tokens, order caches and case records, are encrypted using DPAPI. Operator authentication records and migration recovery archives are also DPAPI-protected. Decryption requires the relevant Windows user profile; no plaintext fallback is available.

Known limits and workstation controls

The complete SQLite file, product tables and media files are not encrypted by the application. Full-disk encryption on the D: drive was not verified. DPAPI does not protect against malware already running as the operator. Do not state that all stored data or all backups are encrypted without independently verifying those additional locations.

In transit and third parties

Use HTTPS for remote API and provider transfers. The local UI uses HTTP on loopback, not a public HTTP endpoint. Send only data necessary for each feature. Do not place order/customer records, credentials or tokens in AI prompts. Product facts and media may be sent to configured AI providers; the exact processing countries depend on provider endpoints and routing and remain to be mapped.

Logging and backups

Do not log secrets, OAuth query strings, cookies or request bodies. The application redacts credential patterns and suppresses verbose HTTP client logs. Create protected backups and test restoration using the same Windows profile. Track copies exported elsewhere; local cleanup does not remove them automatically.

Incident Response and Notification Procedure

Version 1.0 · 13 November 2026 · Proposed; pending operator adoption

Intake and ownership

The operator receives reports at delevedoves@gmail.com and reviews security records whenever operating the app. Register a case under Security > Incident, using a summary without credentials. Record detection time, scope, suspected data categories, actions and status. This is a manual procedure, not an automated threat detection service.

Triage and containment

Triage a new report within one business day as an internal operating target. For suspected active compromise, promptly pause the pipeline, stop affected processes, isolate the workstation if necessary and revoke/rotate affected credentials through official platforms. Preserve relevant evidence without distributing raw tokens or customer data.

Notification workflow

The operator determines affected systems, accounts and parties, and uses the TikTok Shop Partner Center support/review channel for platform-related incidents. Report the known facts, approximate timing, affected data categories, containment and next steps. Follow applicable platform and legal notification requirements; this policy does not invent a universal statutory deadline. Document decisions and communications in the case record.

Recovery and closure

Correct the cause, validate dependencies and controls, restore only a verified backup if appropriate, and reauthorize affected integrations. Test before resuming production. Record resolution and lessons learned, then update the relevant procedure. No absence of historical incidents is asserted by this document.

Vulnerability and Threat Management Procedure

Version 1.0 · 13 November 2026 · Proposed; pending operator adoption

Recurring checks

Run tools/security_check.py and a pip-audit scan monthly, after dependency changes and before a security-sensitive release. Record date, findings, owner, priority and remediation in a Vulnerability case. Validate the Windows antivirus status and updates using its own console; a Windows registration entry alone does not prove current real-time protection.

Risk-based response

Internal remediation targets after triage: critical within 48 hours; high within seven days; medium within 30 days; low within 90 days. If these targets cannot be met, document the reason, affected use, containment and owner decision. Do not resume a feature with an unresolved critical exposure merely to meet a publishing deadline.

Verification and evidence

Install updates from trusted package sources, retain the dependency audit result, and rerun the relevant regression/security tests. A successful advisory scan means no known vulnerabilities were reported by that feed at that time; it is not a penetration test or a guarantee of security.

Initial check

The initial assessment identified a known pip advisory in version 26.1.2. pip was updated to a patched version and the repeated scan reported no known vulnerabilities. The sanitized audit output and dated controls report are stored locally under output/security; they do not establish compliance with all TikTok requirements.

Privacy Requests, Retention and Deletion Procedure

Version 1.0 · 13 November 2026 · Proposed; pending operator adoption

Requests and identity checks

Receive access, correction and deletion requests at delevedoves@gmail.com or through an authenticated official platform channel. Register a Privacy Request case. Confirm identity and authority proportionately before disclosing information, and collect no unnecessary identity documents. The operator handles requests manually and records their outcome. The internal scope does not exempt the integration from platform obligations.

Access and correction

Locate the relevant data, distinguish records controlled by Helios from those controlled by external platforms, and provide only information attributable to the requester. The app offers an operator-only encrypted data export for internal review. Decrypt only in a protected location and minimize/redact the result before a verified disclosure. Correct inaccurate local records and handle platform records through the appropriate platform procedure.

Retention

Application job metadata and security event metadata: 90 days. Order cache without refresh: 90 days. Closed case records: 365 days. Open cases remain until resolved. Product media and video projects remain until explicit operator deletion. Session records expire on logout, replacement or timeout. Any retention exception must have a documented purpose and a review date.

Deletion and termination

The operator may delete the order cache from the Security page with an explicit confirmation. For full local termination, stop the app, run tools/purge_local_data.py in preview mode, verify the scope, then execute with its required confirmation. This deletes local data, credentials and workspace backups. It was tested only in temporary directories and was not executed against production data.

External copies and completion

Track and remove or appropriately handle previous exports, email attachments, cloud/OS backups and copies held by providers separately. Revoke platform access through official controls. Do not claim deletion is complete until all in-scope copies have been checked and applicable retained records are documented. Log the completed actions without retaining the deleted content. This procedure does not promise that local deletion automatically deletes data at third-party services.

Readiness and Evidence Register

Version 1.0 · 13 November 2026 · Proposed; pending operator adoption

Policy publication

Prepared for publication; verify that the public URL is available before declaring publication. Effectiveness depends on recorded owner adoption and continued execution.

Access control

Implementation tested; initial operator password remains to be created on the real installation.

Protection at rest

Secrets, confidential KV caches and auth records: DPAPI. Complete drive/database/media encryption: not verified / not implemented by the app.

Incident and privacy handling

Manual intake channel and protected case register implemented. Operator must adopt the procedure and actually handle reports/requests.

Vulnerabilities

Initial advisory scan completed and pip patched. Monthly checks and response targets require operator follow-through.

Network and endpoints

Windows Firewall profiles were enabled; Kaspersky was registered in Windows Security Center. Current real-time protection, corporate segmentation and workstation lock policy require separate confirmation.

Privacy commitments

Review in up to 90 days after adoption. Local deletion tools do not remove copies at providers or previously exported copies; those require separate tracking.

No unsupported attestations

No DPO appointment, certification, absence of past breaches/complaints, complete processing-country list or TikTok approval is asserted.