Praxio Information Security Policy

Security, access control, data classification, encryption, vulnerability management and incident response

Version 1.0 | Effective date: 6 November 2026 | Next review: no later than 6 November 2027 | Owner: Matheus Martins Abdala (sole operator)

1. Purpose and scope

This policy defines how Praxio protects information and systems. Praxio is an integration service that connects the TikTok Shop stores of Brazilian sellers, through the official TikTok Shop Partner API, to the management applications of those sellers. Praxio is operated by 64.728.974 MATHEUS MARTINS ABDALA (CNPJ 64.728.974/0001-79), a sole-proprietor company (MEI) based in Campo Grande, MS, Brazil. The policy covers all Praxio systems, source code, credentials, devices used to operate the service and all data processed on behalf of sellers.

2. Roles and responsibilities

Praxio is operated by one person, who is accountable for security, access management, incident response and for keeping this policy current. There are no employees or subcontractors with access to production data. If that changes, every person with access will sign a confidentiality agreement and receive access under the rules of section 4 before starting work.

3. Data classification and handling

Class	Examples	Handling rules
Confidential	TikTok Shop access and refresh tokens, app secret, API keys, database credentials, seller financial data, any personal data	Encrypted in transit and at rest. Never written to logs, source code or chat. Access only by the operator and by the service itself. Isolated per seller.
Internal	Product catalog data, order and finance records processed for a seller, system configuration	Encrypted in transit. Shown only to the seller who owns the data. Not shared with third parties.
Public	This policy, the privacy policy, product descriptions of the service	May be published.

4. Access control (least privilege)

- Access to systems, data and credentials is granted only to what is required for the task (least privilege) and is reviewed at least once a year and whenever a person or integration is removed.
- Multi-factor authentication is required on every account that can reach production or source code: email, code repository, DNS and CDN, hosting and deployment panel, and the TikTok Shop Partner Center.
- Each seller's data is logically isolated. Every database query and API call is scoped to the authenticated seller; one seller can never read another seller's data.
- Praxio requests only read-only scopes from TikTok Shop (shop information, product basic, orders and finance). Write scopes are requested only if a seller explicitly asks for a feature that needs them, and changes to a seller's store are performed only after that seller's explicit confirmation.
- Seller applications reach Praxio only with a per-seller API credential that is stored server-side, can be rotated at any time and can be revoked immediately. TikTok tokens are never sent to the seller's application or browser.
- Shared accounts are not used. Passwords are unique, generated and stored in a password manager.

5. Encryption and key management

- All traffic to and from Praxio uses HTTPS (TLS 1.2 or higher). Plain HTTP is redirected or disabled.
- TikTok access and refresh tokens are encrypted at the application level before being stored in the database. Encryption keys and the app secret are held as environment secrets of the hosting platform, outside the source code and outside the database.
- Operator laptops use full-disk encryption. Database backups are encrypted.
- Secrets are rotated when a person with access leaves, after any suspected exposure, and at least once a year.

6. Network and infrastructure security

- Production runs on a dedicated server protected by a host firewall that exposes only the ports required to serve the application over HTTPS. Administrative interfaces and the database are not exposed to the public internet and are reachable only through authenticated, encrypted channels.
- The operating system, container images and runtime are kept up to date. Production and development environments are separate and use separate credentials.
- Application and server logs are retained for troubleshooting and security review. Logs never contain tokens, secrets or full personal data. Unusual activity (failed logins, spikes in requests, unexpected errors) is reviewed and generates an alert to the operator.
- Automated, encrypted backups of the database are kept, and restoration is tested at least twice a year.

7. Endpoint and baseline security

- Devices used to operate Praxio run a supported operating system with automatic updates, active antivirus (Microsoft Defender or equivalent with real-time protection), a host firewall and full-disk encryption.
- Screens lock automatically after a short idle period. Strong, unique passwords and multi-factor authentication are mandatory. Confidential data is not stored on removable media or personal messaging apps.
- A clean-desk and clean-screen practice applies whenever work is done outside the home office.

8. Secure development

- Source code is kept in a private repository. Secrets are never committed. Changes are reviewed by the operator before release and tested before deployment.
- Third-party dependencies are scanned for known vulnerabilities and updated on a regular basis. Critical vulnerabilities are patched within the timelines of section 9.
- Input from sellers and from TikTok webhooks is validated, requests are authenticated and rate limits are applied to protect the service and to respect TikTok API limits.

9. Vulnerability and threat management

Severity	Examples	Target time to fix or mitigate
Critical	Remote code execution, exposed secrets, authentication bypass	Within 24 hours
High	Data exposure between sellers, privilege escalation	Within 7 days
Medium	Missing hardening, outdated library with limited exposure	Within 30 days
Low	Minor configuration or informational findings	Next scheduled maintenance

The operator monitors security advisories for the runtime, frameworks and hosting stack in use, reviews dependency alerts at least weekly and records each finding and its resolution.

10. Incident response

A security incident is any event that compromises, or is reasonably suspected to compromise, the confidentiality, integrity or availability of Praxio systems or seller data.

Step	Action	Owner
1. Detect and report	Anyone who notices an incident reports it immediately to matheusmabdala@gmail.com. The operator opens an incident record with time, scope and evidence.	Operator
2. Contain	Revoke or rotate affected credentials and tokens, isolate affected systems, preserve logs.	Operator
3. Assess	Determine which sellers and which data are affected and classify severity.	Operator
4. Notify	Notify affected sellers and TikTok Shop without undue delay and no later than 72 hours after confirming that personal data was affected. Notify the Brazilian data protection authority (ANPD) and data subjects when required by law (LGPD).	Operator
5. Recover	Restore services from clean backups, fix the root cause and verify before resuming.	Operator
6. Review	Within 14 days, document the cause, impact and actions, and update controls and this policy.	Operator

Sellers and TikTok Shop can report suspected incidents at any time to matheusmabdala@gmail.com.

11. Data retention and deletion

Praxio keeps seller data only for as long as needed to provide the contracted service. When a seller revokes authorization or the contract ends, the seller's tokens are deleted immediately and the remaining seller data is deleted within 30 days. Encrypted backups containing that data expire within 35 days. Sellers can request deletion, correction or a copy of their data at any time at matheusmabdala@gmail.com.

12. Third parties and sub-processors

Praxio uses a commercial hosting provider for servers, a DNS and CDN provider, and the official TikTok Shop Partner API. Providers are chosen for security and reliability, are used only to deliver the service, and are reviewed at least annually. A current list is available on request.

13. Awareness, review and exceptions

The operator reviews this policy at least once a year and after any significant incident or change to the service. Exceptions must be recorded with a reason, a risk assessment and an end date.

14. Contact

Security and privacy contact: Matheus Martins Abdala, matheusmabdala@gmail.com. Company: 64.728.974 MATHEUS MARTINS ABDALA, CNPJ 64.728.974/0001-79, Campo Grande, MS, Brazil.