marguno.

Information security policy

Version 1.0 | Effective 24 November 2026

Ownership and scope

Aldergo Menezes da Silva, the Marguno operator, maintains this policy and coordinates incident response. It covers the web application, administrative computers, infrastructure accounts and data received from authorized shops.

Access and devices

Operators must use individual credentials, limit access to their assigned duties and enable multifactor authentication on administrative accounts that support it. Computers with administrative access must use screen locking, security updates and real-time antimalware protection. Access must be reviewed when duties change or access is no longer needed.

Data and credentials

Customer information and shop identifiers may be accessed only for an authorized purpose. Secrets and tokens require additional protection. The TikTok Shop integration uses HTTPS and encrypts authorization credentials before storage. Operators must use fictitious data in demonstrations and keep passwords, tokens and personal data out of diagnostic records and support tickets.

Changes and providers

Before releasing a change, the operator must assess its effects on permissions and data, test it and identify a recovery method. When adding an integration or provider, the operator must assess its purpose, access and processing locations. Security advisories must be evaluated according to exposure and impact.

Reporting and response

Report suspected unauthorized access, data exposure or device loss to contatomarguno@gmail.com. Identify the affected service, approximate time and what you observed. The operator must record the report, contain the exposure, preserve relevant evidence and assess notification to merchants, the marketplace and authorities under applicable obligations.

Review and publication

The operator will review this policy at least annually and after material changes or incidents. The current version is available at this public address to operators, merchants and partners.