ZAP BRABO
TECHNOLOGY LTDA · CNPJ 66.000.756/0001-49

Goiânia, Goiás, Brazil
zapbrabo.com
contato@zapbrabo.com

Information Security Policy

Version 1.1 · Effective 12 August 2026 · Public document

Document	Information Security Policy (ISP)
Version	1.1
Effective date	12 August 2026
Next review	12 August 2027 (or upon material change)
Owner	Security Officer
Classification	Public

1. Purpose

This policy defines the information security and privacy program of ZAP BRABO TECHNOLOGY LTDA ("ZapBrabo") and the controls applied to protect the confidentiality, integrity and availability of the data we process — including data received from partner platforms and personal data belonging to our clients and to their customers.

It is written to satisfy, in a single document, the security program requirements of the commerce and messaging platforms we integrate with, and to comply with Brazilian Law No. 13.709/2018 (LGPD).

2. Scope

This policy applies to all systems, environments, personnel and third parties involved in operating the ZapBrabo platform. In scope:

- The production application (Laravel/PHP) and its database
- The production server and network perimeter
- Source code repositories and the deployment pipeline
- Administrative interfaces and credentials
- All data received from integrated platforms via API or webhook

3. Organisation and responsibilities

ZapBrabo is a small technology company. In accordance with the principle that a security program must be **appropriate to the nature, size and complexity of the business**, responsibilities are consolidated as follows:

Security Officer — Murilo Martins, Founder and Technical Lead. Accountable for this policy, for the security program, for incident response, and for communication with partner platforms on security matters. Contact: `contato@zapbrabo.com`

Any change to the Security Officer or to the security contact is communicated to affected partner platforms within the timeframe each platform requires.

All personnel with access to production systems must read and accept this policy before access is granted, and access is revoked within 24 hours of the cessation of the need for such access.

4. Data classification

Class	Examples	Handling
Restricted	Access tokens, API secrets, passwords, customer tax IDs (CPF/CNPJ)	Encrypted at rest, never logged, never transmitted outside TLS, access limited to the Security Officer
Confidential	End-customer conversations, contact records, order data, platform-provided data	Encrypted in transit, logically segregated per tenant, retention-limited
Internal	Application logs, operational metrics	No personal data retained beyond the defined retention period
Public	Marketing site, this policy, terms and privacy notice	No restriction

Data received from partner platforms is treated as **Confidential** or **Restricted** depending on content, is never used for any purpose other than providing the contracted service, and is never sold, shared or used to train third-party models.

5. Access control

- Administrative access to the platform requires authentication against a credential stored as a one-way bcrypt hash. Plaintext passwords are never stored.
- Access follows the principle of **least privilege**: each tenant's users can access only their own tenant's data, enforced at the application query layer by mandatory tenant scoping.
- Authentication endpoints are rate limited to 5 attempts per minute per source address to mitigate credential stuffing and brute force.
- Administrative endpoints, public API endpoints, webhook endpoints and AI-processing endpoints each carry independent rate limits.

- **Platform reviewers receive scoped, read-only accounts.** Where a commerce or messaging platform requires access to assess the application, we issue a dedicated account that is restricted to a single demonstration tenant and rejects every state-changing request. Administrative credentials are never shared with third parties. Each reviewer account is issued per platform, logged on use, and revocable independently.
- Production credentials are held exclusively in server-side environment configuration. They are excluded from version control by policy and by repository configuration, and are never transmitted through chat, email or ticketing systems.

6. Network and infrastructure security

- The production environment runs on Ubuntu Server LTS hosted by DigitalOcean, a provider operating data centres under recognised security certifications. Physical security of the facilities is inherited from the provider.
- A host firewall (`ufw`) enforces default-deny inbound, permitting only the ports required to operate the service.
- An intrusion prevention agent (`fail2ban`) monitors authentication and service logs and automatically blocks source addresses exhibiting brute-force or abusive patterns.
- All external traffic is served over **TLS 1.2 or above**. Certificates are issued by a public certificate authority and renewed automatically.
- Anti-malware scanning is installed on the production server, with signature definitions updated automatically and scheduled filesystem scans of the application, administrative and temporary directories.
- All HTTP responses carry security headers: HTTP Strict Transport Security, X-Content-Type-Options, X-Frame-Options, Referrer-Policy and Permissions-Policy.
- Operating system and package security updates are applied on a schedule weighted by severity; critical patches are applied as soon as practicable.

7. Encryption

- **In transit:** TLS 1.2+ for all public traffic and for all outbound calls to partner platform APIs. Credentials are transmitted only in Authorization headers over TLS.
- **At rest:** all third-party access tokens and refresh tokens, all payment provider API keys, all webhook secrets, and end-customer tax identifiers are encrypted at the application layer using AES-256-CBC with an application key held only in server-side environment configuration.
- **Passwords:** stored exclusively as salted one-way hashes (bcrypt). Password recovery never discloses an existing password.

8. Application security

- All source code is version controlled. Every change is committed with an attributable author and a description, giving a complete and auditable change history.

- The application is built on a maintained major version of the Laravel framework, which provides parameterised database access (mitigating SQL injection), output escaping by default (mitigating cross-site scripting) and CSRF tokens on state-changing requests.
- Inbound webhooks are authenticated. Requests that fail signature or token verification are rejected before any processing occurs.
- Dependencies are managed through lockfiles, giving deterministic builds and a reviewable dependency inventory.
- Actions taken on behalf of a client that would be publicly visible or financially material require explicit human approval before execution. No automated process publishes content or spends funds in a client's name without that approval.

9. Logging and monitoring

- The application records security-relevant events, including authentication outcomes, administrative actions, integration authorisations, and every outbound API call with its endpoint, purpose and HTTP status.
- **Application logs do not contain personal data.** A redaction layer applied at the logging channel removes telephone numbers, e-mail addresses, tax identifiers, access tokens and secrets from every log entry — both from structured fields and from free text — before it is written to disk. Only the last four characters of an identifier are preserved, which is enough to correlate with a database record during an investigation but not enough to identify or contact a person.
- Logs are rotated daily, compressed and **retained for 90 days**, with filesystem permissions restricting access to the operating system administrator.
- Failures in integration flows are logged with sufficient context to investigate, and are reviewed when an anomaly is reported.

10. Data retention and disposal

- Personal data is retained only for as long as necessary to provide the contracted service, and in any case **no longer than 90 days** after it ceases to be necessary, except where a longer period is required by applicable law.
- **This limit is enforced automatically.** A scheduled job runs daily and removes conversations, messages and contact records that fall outside the retention window. Records subject to a statutory retention period under Brazilian tax and consumer law — orders and payments — are preserved, as are contacts with future appointments. Each execution is recorded in the application log as evidence that the control operates.
- Upon termination of a client relationship, or upon a valid deletion request from a partner platform, the corresponding data is removed from production within 30 days.
- Data subjects may exercise their LGPD rights — access, correction, deletion, portability — through `contato@zapbrabo.com`, as published in our Privacy Notice.
- Disposal renders data unreadable and unrecoverable.

11. Incident response

An information security incident is any actual or suspected unauthorised access to, disclosure of, alteration of or loss of data under our control.

1. **Detect and contain.** On detection, the Security Officer immediately takes measures to limit the impact, including revoking credentials, blocking access and isolating affected components.
2. **Notify.** Affected partner platforms are notified through the channel and within the deadline each platform requires — **and in any event no later than 24 hours** from becoming aware, when the platform specifies that deadline. The Brazilian National Data Protection Authority (ANPD) and affected data subjects are notified where LGPD requires it.
3. **Investigate.** Evidence, including relevant logs, is preserved for the duration of the investigation and for as long as any partner platform requires.
4. **Report.** A written report is produced describing the extent of the incident, the data involved, the corrective actions taken and the measures adopted to prevent recurrence.
5. **Remediate.** Root causes are addressed and this policy is updated where the incident reveals a gap.

12. Third parties and sub-processors

ZapBrabo uses the following categories of sub-processor. Each is bound by its own terms and, where personal data is processed, by obligations no less restrictive than those in this policy:

Sub-processor	Purpose	Location
DigitalOcean LLC	Application hosting and infrastructure	United States
Meta Platforms, Inc.	WhatsApp Business Platform messaging	United States
Anthropic PBC	AI language processing	United States
OpenAI, L.L.C.	AI language and speech processing	United States
Asaas Gestao Financeira S.A.	Payment processing	Brazil

Data received from a commerce platform is **never** transmitted to another commerce platform, and is logically segregated per tenant so that no client can access another client's data.

13. Business continuity

Source code is replicated in a remote version control repository, allowing the application to be rebuilt from a known state. Infrastructure is reproducible from documented provisioning procedures. Recovery objectives are set in proportion to the service level committed to clients.

14. Policy governance

This policy is reviewed at least annually and whenever there is a material change to our systems, to the data we process, or to the requirements of a partner platform. Material changes affecting the security of partner-provided data are communicated to affected platforms in writing within the timeframe each platform requires.

15. Continuous improvement programme

Consistent with a security program proportionate to our size, the following controls are formally scheduled. This section is published as part of the policy in the interest of transparency.

Implemented on 12 August 2026:

Control	Status
Automated enforcement of the 90-day personal data retention limit	Implemented
Redaction of personal identifiers from application logs	Implemented
90-day log retention with rotation and compression	Implemented
HTTP security headers (HSTS and four others)	Implemented
Endpoint anti-malware with scheduled scanning	Implemented
Scoped, read-only reviewer accounts for platform assessors	Implemented

Scheduled:

Control	Target
Public-key-only SSH authentication; password authentication disabled	Q3 2026
Off-site encrypted database backups with restore testing	Q3 2026
Content-Security-Policy header	Q4 2026
Quarterly internal and external vulnerability scanning	Q4 2026
Independent application security assessment	Subject to platform requirement

Approved by

Murilo Martins — Founder and Security Officer ZAP BRABO TECHNOLOGY LTDA 12 August 2026 (v1.1)

Published at zapbrabo.com. This policy is a public document and may be shared with partner platforms, clients and auditors.