Security Policy

RWS Ltda. · CNPJ 46.231.982/0001-23 · Av. Santo Amaro, 1047 · São Paulo/SP, Brazil

Security contact: security@rwsintegration.com · Data Protection Officer (DPO): dpo@rwsintegration.com

This document describes the security architecture, the isolation and the compliance of the RWS integration infrastructure across the entire data life cycle: receipt, processing and delivery. It complements the "Compliance and Security Document: Site-to-Site Connection", which details VPN connectivity with customer environments, and is incorporated by reference into the Data Processing Addendum (DPA), published at rwsintegration.com/pt-br/legal/dpa (English version at rwsintegration.com/en/legal/dpa), as its Security Policy.

CONTENTS

1. Data Centers and Physical Security
2. Network Security
3. Architecture and Multi-Tenant Isolation
4. Secrets and Credentials Management
5. Encryption
6. Availability and Continuity
7. Application Security (SDLC)
8. Penetration Testing and Vulnerability Assessments
9. Security Incident Response
10. Monitoring, Logs and Auditing
11. Organization and People
12. Privacy and Data Protection (LGPD)
13. Certifications and Additional Documentation

1. Data Centers and Physical Security

NAME	DETAILS
Facilities	The physical infrastructure of the RWS platform is hosted and managed in the secure data centers of Amazon Web Services (AWS). RWS does not operate its own physical servers or data centers: the entire physical and infrastructure layer is inherited from AWS, which

NAME	DETAILS
	manages risks continuously and undergoes recurring independent assessments. AWS data center operations are accredited under: ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 1 and SOC 2, and PCI DSS. (See Section 13, Certifications and Additional Documentation.)
Physical Security	AWS data centers have perimeter control, video surveillance, intrusion detection systems and strictly controlled physical access, with multi-factor authentication for authorized personnel and continuous escort of visitors. Public details at aws.amazon.com/compliance/data-center/controls.
Location	The data processed by the platform is stored and processed in the us-east-1 region (AWS, United States). The international transfer of data takes place under the safeguards of art. 33 of the LGPD (Law 13,709/2018), through the standard contractual clauses approved by the ANPD entered into between RWS and AWS, as set out in Annex IV of the DPA.

2. Network Security

NAME	DETAILS
Security Response Team	The RWS security team responds to security alerts and events and can be contacted at security@rwsintegration.com.
Network Isolation	The core of the platform runs in a private, isolated VPC, with no inbound access from the internet. All traffic is exclusively outbound, originated by the platform itself (the same principle applied to Site-to-Site connections). There is no public exposure of IPs of the processing environment, nor reverse NAT; return routes are restricted to responses to connections initiated by the platform.
Protection (Firewalls)	The private subnets are protected by Network ACLs and Security Groups with a deny-by-default policy: only explicitly authorized destinations, ports and protocols are allowed, assigned by the function of each workload.
Public Endpoints	The public components (webhooks and receiving APIs) are exposed exclusively via AWS API Gateway, with authentication, rate limiting and throttling, and traffic protected by HTTPS/TLS 1.2+. The webhook component has minimal authorization: its only permission is to write the received data to the extraction queue. There is no network path from the public endpoint to the internal environment: communication happens exclusively through queues. Even in case of abuse of the public endpoint, the attack surface is limited to the receiving layer.

NAME	DETAILS
DDoS Mitigation	The public endpoints are protected by AWS Shield Standard (automatic mitigation of network and transport layer attacks), combined with throttling at the API Gateway. The asynchronous, queue-driven design absorbs traffic spikes without impact on the processing environment.
Network Monitoring	Network traffic is monitored through VPC Flow Logs and CloudWatch, with automatic anomaly alerts.
Logical Access	Access to the production network is restricted on a need-to-know basis, with individual, named accounts, least privilege and multi-factor authentication (MFA). (See Section 11, Organization and People.)

3. Architecture and Multi-Tenant Isolation

NAME	DETAILS
Architecture	The platform is built entirely on AWS managed and serverless services (ECS Fargate, Lambda, managed queues and storage), operating in multiple availability zones (multi-AZ). Processing is asynchronous and queue-driven: transient failures result in automatic reprocessing, not in data loss.
Delivery Semantics	The platform guarantees exactly-once delivery: each integration record is processed and delivered exactly once, with per-record completion control; automatic reprocessing does not generate duplication.
Infrastructure as Code	The environment is provisioned and updated exclusively through infrastructure as code (IaC), via automated pipelines, keeping the configuration consistent, versioned and auditable. There are no manual infrastructure changes.
Isolation per Integration	Each integration runs on fully isolated compute and queues. Distinct executions do not share processing context.
Isolation between Customers	Data of different customers never crosses: there is no reuse of workloads, queues or context between tenants.
Least Privilege	The permissions of each workload follow the least privilege principle (IAM Policies), with access restricted exclusively to the resources of the customer and of the execution itself.

4. Secrets and Credentials Management

RWS

NAME	DETAILS
Storage	All credentials (APIs, databases, VPNs and customer systems) are stored in AWS Secrets Manager, with encryption at rest (AES-256).
Segregation per Tenant	Each customer (tenant) has its own segregated secrets vault. There is no shared credentials repository between customers.
Runtime Injection	Secrets are injected exclusively at runtime into the authorized workload. They are never written to source code, configuration files or logs.
Human Access	Human access to customer secrets is restricted, audited and is not part of the day-to-day operation of the platform.

5. Encryption

POLICY	DETAILS
Encryption in Transit	All external communication uses HTTPS/TLS 1.2+ (public endpoints and API integrations). Site-to-Site VPN connections use IPsec with AES-256.
Encryption at Rest	Data at rest is encrypted with AES-256, through AWS managed encryption (SSE), in databases, queues, object storage and logs. RWS does not implement proprietary cryptography: it uses exclusively certified cryptographic mechanisms managed by AWS.
Backup Encryption	Database backups are performed through automated snapshots, encrypted with AES-256, with a controlled retention period. Transient processing storage (cache and queues) does not retain data durably and operates with the native redundancy of the AWS managed services.

6. Availability and Continuity

POLICY	DETAILS
Availability SLA	RWS contractually commits to a target monthly availability of 99.90%, with service credits (progressive discounts on the subscription) in case of non-compliance, as set out in the Order Form. Availability is monitored continuously.
Processing SLA	Target processing time for integration data (receipt → delivery) of up to 15 minutes, sustained by automatic autoscaling of processing capacity. Exception: integrations with sources or destinations subject to rate limiting imposed by the external system may exceed this target, respecting the third party's limits.

POLICY	DETAILS
Redundancy	The managed services operate in multiple availability zones (multi-AZ), eliminating single points of failure at the infrastructure layer.
Failure Resilience	Queue-driven processing ensures that transient failures result in automatic reprocessing, not in data loss.
Disaster Recovery	Encrypted snapshots and controlled retention allow data restoration; infrastructure as code allows the complete and consistent re-provisioning of the environment.

7. Application Security (SDLC)

POLICY	DETAILS
Code Review	All code goes through mandatory review via pull request before being merged. No code is deployed without review.
CI/CD Pipeline	Production deployments happen exclusively through an automated pipeline (CI/CD), with mandatory quality gates: static analysis (lint), type checking, automated tests and build. Pipeline credentials are segregated and least-privilege.
Dependency Analysis	Third-party dependencies are continuously checked for known vulnerabilities (CVEs), with updates prioritized by severity. New dependency versions go through a quarantine period before being adopted, mitigating supply chain attacks.
Environment Segregation	The staging and production environments are fully segregated (distinct credentials, queues, databases and compute). The staging environment operates under the same isolation and access controls as the production environment.

8. Penetration Testing and Vulnerability Assessments

POLICY	DETAILS
Internal Assessments	RWS conducts periodic assessments of the security posture of the environment, based on best practices and AWS native tools. Findings are classified by risk and addressed with corresponding priority.
Third-Party Testing	Security tests of the RWS services may be performed by independent consulting firms engaged by the customer, upon RWS's prior written authorization, as provided for in the agreement. The findings of each assessment are reviewed jointly, classified by risk and assigned to the responsible team for resolution under SLA. The costs of these tests are borne by the customer.

RWS

9. Security Incident Response

POLICY	DETAILS
Process	In the event of an incident, the RWS engineering team is engaged to collect and analyze logs of the affected systems (distributed tracing, structured logs and audit trails) and respond in the most appropriate way. Responsibilities between RWS and AWS follow the shared responsibility model, under the coordination of the RWS team.
Response Times	Target response times are contractually committed: critical incidents within 2 hours (business hours) and 8 hours (weekends and holidays); non-critical incidents and support requests within 2 business days, with service credits in case of non-compliance.
Customer Notification	Security incidents involving personal data are communicated to the customer (Controller) within the time limits and in the manner of Section 6 of the DPA and art. 48 of the LGPD, with RWS supporting the customer in any communications to the ANPD.
Contact	Events and suspected incidents can be reported to security@rwsintegration.com.

10. Monitoring, Logs and Auditing

POLICY	DETAILS
Observability	The platform is instrumented with distributed tracing and metrics (OpenTelemetry), centralized in the RWS observability stack.
Execution Logs	Each integration execution generates structured logs, with business-level error visibility made available to the customer on the platform itself.
Administrative Auditing	Administrative actions in the AWS environment are audited via AWS CloudTrail.
Retention	Execution logs are retained for 90 days, with encryption at rest (AES-256), used exclusively for diagnostics and support purposes, with restricted access. The logs may contain the payloads processed by the integrations. Secrets and credentials are masked by default, and the customer can configure the masking of the personal data fields that should not appear in the logs, according to its own assessment of necessity. Backups follow retention controlled by data type.

11. Organization and People

METHODOLOGY	DETAILS
Security Policies	RWS maintains internal information security policies, shared with all employees and contractors with access to information assets.
Training	All engineers go through security onboarding, covering the secure development, secrets management and data protection (LGPD) practices adopted by the platform, with periodic reinforcement.
Confidentiality	All employees and contractors with access to customer information are bound by confidentiality agreements, with obligations equivalent to those assumed by RWS toward its customers (Section 10 of the MSA).
Infrastructure Access	The team has no direct access to the AWS environment: permanent access is restricted to the technical leadership (CEO and CTO), and every infrastructure change happens exclusively through infrastructure as code, reviewed and auditable. During incidents, engineers receive temporary credentials (IAM sessions with a defined duration), automatically revoked upon expiration.
Corporate Access Control	Access to the environments follows the least privilege principle, with individual, named accounts (shared accounts are prohibited) and mandatory MFA on the infrastructure administration systems.
Revocation and Review	Administrative access to production is restricted to the engineering team responsible for operations and revoked immediately upon termination. Periodic access reviews are conducted by the RWS Security Officer.

12. Privacy and Data Protection (LGPD)

POLICY	DETAILS
Roles	RWS acts as Processor of personal data, processing data exclusively in accordance with the instructions and for the purposes contracted by its customers (Controllers), under the Terms of use (rwsintegration.com/pt-br/legal/terms, English version at rwsintegration.com/en/legal/terms) and the Data Processing Addendum (DPA, rwsintegration.com/pt-br/legal/dpa, English version at rwsintegration.com/en/legal/dpa).
Data Protection Officer (DPO)	RWS has appointed a Data Protection Officer, the communication channel with Data Subjects and with the ANPD: dpo@rwsintegration.com.
Data Categories	The categories of personal data that may pass through the integrations (including identification data such as CPF, bank account data and, where necessary for the integration, sensitive personal data)

POLICY	DETAILS
	are defined in Annex I of the DPA. The customer decides which fields pass through each integration.
Purpose Limitation	Customer Content is used exclusively to provide and maintain the contracted service. Usage data may be used for service maintenance and improvement only in aggregated and de-identified form, as set out in the MSA, with the obligations regarding Personal Data under the Applicable Data Protection Laws fully preserved. Customer data is never sold or shared with third parties, in any form.
Retention and Deletion	Upon termination of the agreement, Customer Content is deleted within 60 days upon request, and Confidential Information is returned or destroyed, as set out in the MSA. During the term, logs and backups follow controlled retention.
International Transfer	See Section 1 (Location): safeguards of art. 33 of the LGPD, contractual clauses and the AWS data processing terms.
Sub-processors	The list of sub-processors, with the purpose, data processed, location and transfer mechanism of each one, is published at rwsintegration.com/pt-br/legal/subprocessors (English version at rwsintegration.com/en/legal/subprocessors). Changes are communicated to customers as set out in Section 3 of the DPA.
Incidents involving Personal Data	Communicated as set out in Section 9 (Incident Response) and art. 48 of the LGPD.
Public Documents	Terms of use: rwsintegration.com/pt-br/legal/terms · Privacy policy: rwsintegration.com/pt-br/legal/privacy · DPA: rwsintegration.com/pt-br/legal/dpa · Sub-processors: rwsintegration.com/pt-br/legal/subprocessors

13. Certifications and Additional Documentation

CERTIFICATION / DOCUMENT	DETAILS
Shared Responsibility	Platform security follows the shared responsibility model: AWS is responsible for the security of the cloud (physical infrastructure, network, hypervisor), certified under the programs below; RWS is responsible for security in the cloud (architecture, isolation, encryption, access and operations), described in Sections 2 to 11 of this document.
AWS Certifications	The infrastructure used by RWS inherits the AWS certifications: ISO/IEC 27001 (Information Security Management), ISO/IEC 27017 (Cloud Security), ISO/IEC 27018 (Protection of Personal Data in the Cloud), SOC 1 and SOC 2 (Security, Availability and Confidentiality)

CERTIFICATION / DOCUMENT	DETAILS
	and PCI DSS. Issued by independent bodies: aws.amazon.com/compliance/programs
Customer Testing	Customers may engage independent security assessments as set out in Section 8 (Penetration Testing).
Available Documents	Public: this Security Policy, the Terms of use, the DPA, the sub-processors list and the Privacy policy, at rwsintegration.com/pt-br/legal (English versions at rwsintegration.com/en/legal). Upon request and NDA: the Site-to-Site Connection Compliance and Security Document. Contact: security@rwsintegration.com.

Version history

Version	Date	Change
3.0 (current)	June 2026	Renamed to Security Policy; references to the DPA and to the sub-processors page; content of the execution logs
2.0	June 2026	Version initially published under the title Panorama de Segurança (Security Overview)

Legal documents

Terms of use
Privacy policy
Data Processing Addendum (DPA)
Security Policy
Sub-processors

Last updated: June 2026

This English version is provided for convenience only. The Portuguese version at rwsintegration.com/pt-br/legal/security is the official version and prevails in case of any divergence.