



Push-to-talk solution

CORPORATE AND CONTRACTUAL DOCUMENTATION

corePTT Hosting and Server Management Policy

Shared and dedicated environments and operational responsibilities

corePTT platform

Compliance and governance

Security and data protection

15

corePTT governance

Revision 1.3 • 14 October 2026

sales@coreptt.com

COREPTT TECNOLOGIA LTDA

CNPJ 69.599.966/0001-93 • Campinas SP

Revision 1.3 | 14 October 2026

DRAFT FOR LEGAL REVIEW

corePTT Hosting and Server Management Policy

Shared and dedicated environments and operational responsibilities

PROVIDER	COREPTT TECNOLOGIA LTDA
Trade name	COREPTT TECNOLOGIA
CNPJ	69.599.966/0001-93
Registered office	Rua Comendador Torlogo Dauntre, nº 74, sala 1207, Cambuí, Campinas/SP, CEP 13025-270
Brand and platform	corePTT
Revision	1.3
Revision date	14/10/2026
Status	Draft for legal review
Sales channel	sales@coreptt.com (11) 9839-0601
Legal privacy and integrity	legal@coreptt.com

This policy defines how the PROVIDER administers the layers it undertakes, distinguishes shared and dedicated environments and documents CUSTOMER and service provider responsibilities. The free trial follows its own duration and conditions, separate from commercial service levels.

This Policy describes corePTT hosting models and the server and technical component management responsibilities undertaken by the PROVIDER.

Company identification and version control

COREPTT TECNOLOGIA LTDA, trading as COREPTT TECNOLOGIA, registered with CNPJ under No. 69.599.966/0001-93, with its registered office at Rua Comendador Torlogo Dauntre, nº 74, sala 1207, Cambuí, Campinas/SP, CEP 13025-270, is the PROVIDER responsible for the offering and the commitments undertaken in this instrument.

Sales and contracting: sales@coreptt.com; telephone (11) 9839-0601. Legal, privacy and integrity: legal@coreptt.com. The CUSTOMER or evaluating organization shall be identified in the specific instrument by a representative authorized to accept it.

This document is revision 1.3, dated 14/10/2026, and is a draft for legal review. Incorporation requires that its title, version and date be made available and identified before acceptance. Changes to scope or obligations require the applicable record and acceptance; future versions shall not be incorporated automatically and no retroactive unilateral changes shall apply.

1 Environment models

Model	Characteristics	Point to consider
-------	-----------------	-------------------

Shared	common resources with logical segregation between CUSTOMERS	does not mean an exclusive physical machine
Dedicated	listed resources reserved for the CUSTOMER	network, control or cloud services may remain shared
Co-managed	responsibilities divided between the PROVIDER and the CUSTOMER	an access and change matrix is mandatory
In the CUSTOMER's environment	infrastructure supplied or contracted by the CUSTOMER	the PROVIDER manages only the specified layers
Evaluation	temporary free environment for 7 calendar days and 168 hours from the notified activation	without guaranteed commercial SLA, production, backup or restoration, unless specifically committed

2 Service managed by the PROVIDER

When contracted as a managed service, the PROVIDER's service may cover provisioning, secure configuration, administrative control, updating, observability, capacity, backup, restoration, maintenance, incident response and deactivation. The specific extent shall be defined by layer in the accepted schedule and instrument; items not included do not constitute a commercial commitment.

3 Responsibility matrix

Layer or activity	PROVIDER	CUSTOMER or third party
Datacenter or physical cloud infrastructure	coordinates supplier when included	provider operates its infrastructure
Virtual machine or server	manages when contracted	CUSTOMER approves capacity and cost
Operating system	configures and updates when included	CUSTOMER discloses dependencies and windows
corePTT database and application	operates, monitors and maintains	CUSTOMER administers usage and data
Integrations	maintains contracted connectors	external rights holder maintains API, license and service
User network and internet	supports diagnosis	CUSTOMER and telecommunications operator maintain connectivity
Terminals and radios	supports models within scope	CUSTOMER protects, updates and provides
Identities and permissions	provides administrative controls	CUSTOMER authorizes users and reviews access

4 Shared infrastructure

The PROVIDER adopts logical segregation, permissions, tenant identification and controls proportionate to risk. Capacity is managed on an aggregate basis and may be adjusted to maintain stability. Requirements for physical isolation, an exclusive key, a private network or a specific region must be contracted.

5 Dedicated infrastructure

The dedicated designation applies only to the listed resources. It does not automatically imply exclusive physical hardware, an exclusive team, an exclusive connection or the absence of shared provider services. Sizing, redundancy, licenses, region, addressing and administrative access must be recorded in the Order Form.

6 Security and administrative access

- privileged access must be individual, restricted by role and revoked when no longer necessary;
- credentials and secrets must be protected and must not be shared through insecure channels;
- material changes must have authorization, a record and a plan compatible with the risk;
- vulnerabilities and updates shall be handled according to criticality, compatibility and the operational window;
- logs and evidence shall have restricted access and retention appropriate to the purpose and contract.

7 Updating and maintenance

The PROVIDER shall plan updates to managed layers and may perform emergency fixes to reduce a material risk, recording the intervention and communicating foreseeable impacts where possible. Scheduled interventions shall follow the accepted commercial SLA and window where these exist. During the trial, maintenance does not create an SLA or 24 hour service. The CUSTOMER shall participate in testing integrations, firmware and processes dependent on the version.

8 Monitoring and capacity

Metrics, alerts, limits and monitoring hours depend on the plan. The PROVIDER shall handle alerts from the managed layer and propose expansion when there is a trend toward saturation. Increases in users, traffic, storage, integrations or retention may require resizing and a quotation accepted in advance; additional capacity shall not be charged automatically.

9 Backup retention and recovery

The Backup Retention and Deletion Policy supplements this document if identified and accepted during contracting. Retention of recordings for up to 90 days is a commercial commitment only where expressly contracted; other categories have their own periods. Copying frequency, backup retention, testing, RPO, RTO and restoration constitute commitments only when defined in the plan or Order Form. The free evaluation does not guarantee these features.

10 Third parties and subprocessors

The PROVIDER may use cloud, datacenter, communications, monitoring and security providers with the minimum necessary access and confidentiality and data protection obligations. It is responsible for selection, instructions, configuration and supervision compatible with the service it undertakes; division of layers does not exclude its legal or contractual obligations. The list of service providers and subprocessors, the environment, processing countries and mechanism for any international transfer shall be disclosed and

validated before activation in accordance with the DPA and applicable legislation. This policy does not claim certification, datacenter tier or technical compliance without specific substantiation.

11 Incidents and continuity

The PROVIDER shall perform triage, containment, recovery and communication within the layers it undertakes according to its role and severity. The CUSTOMER and service providers shall cooperate and preserve evidence. An incident involving personal data shall be notified between the parties without undue delay, with available information and updates; the controller shall assess notifications to the authority and data subjects when required, within statutory deadlines, with the processor's cooperation and without excluding their own obligations. Commercial contingency, redundancy and disaster recovery depend on the contracted design; during the trial, the CUSTOMER shall maintain its own alternative means.

12 Termination and transition

Upon termination, the PROVIDER shall deactivate access and resources under its management and return, delete or anonymize data according to accepted instruments and lawful instructions. Export, portability, migration and assistance must be agreed before termination; additional services shall require a quotation accepted in advance. Subsequent dashboard access and recovery of deleted content are not guaranteed.

In the free trial of 7 calendar days, equivalent to 168 hours from the notified activation, there is no automatic renewal or conversion to a paid plan. Continuation requires an accepted proposal and formal contract through sales@coreptt.com or (11) 9839-0601. Without a contract or lawful preservation, operational content shall be deleted or anonymized within 30 days after the end and residual backups purged within 90 days after the end, without operational reuse; the periods must be validated against the architecture before signing. Minimum records for statutory retention may remain with restricted access and a limited purpose.

13 Environment schedule

Field	Definition
Model	shared [] dedicated [] co-managed [] CUSTOMER [] evaluation []
Provider and region	_____
Resources and capacity	_____
Layers managed by the PROVIDER	_____
Layers outside scope	_____
Administrative access	_____
Monitoring	_____
Maintenance window	_____
Backup RPO and RTO	_____

Field	Definition
Retention of recordings and other categories	contracted period by category and limit: _____
Incident contacts	_____
Processing countries and subprocessors	_____
International transfer and mechanism	no ☐ yes ☐ validated mechanism: _____
Versions and resource limits	_____
Contingency and prior export	_____
Termination and deletion periods	_____
Architecture and persons responsible for validation	_____

14 Changes and precedence

A change in model, provider, region, capacity, retention or responsibility requires a risk assessment, a record and the relevant approvals; commercial impacts require acceptance. The Order Form defines the commercial environment, the SLA its service levels, the DPA personal data and the Enterprise Agreement the general rules. During the free evaluation, the accepted 07 Day Evaluation Agreement and activation schedule prevail for their specific scope. All incorporated instruments shall be identified by title, version and date before acceptance, without retroactive unilateral changes.

Document control

Field	Record
Editorial ownership and maintenance	COREPTT TECNOLOGIA LTDA
Approval authority	Authorized representative to be identified upon acceptance
Sales channel	sales@coreptt.com
Legal privacy and integrity	legal@coreptt.com