



Push-to-talk solution

CORPORATE AND CONTRACTUAL DOCUMENTATION

corePTT Security and Trust

Governance controls shared responsibility and incidents

corePTT platform

Compliance and governance
Security and data protection

06

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 Security and Trust

Governance controls shared responsibility and incidents

Responsible 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
Sales and contracting	sales@coreptt.com
Registered telephone	(11) 9839-0601
Legal matters privacy and integrity	legal@coreptt.com
Brand and platform	corePTT
Revision	1.3
Revision date	14 October 2026

This document presents verifiable security commitments and distinguishes the controls of the PROVIDER, the CUSTOMER, users, telecommunications operators and suppliers.

This document establishes the security controls and responsibilities for corePTT, coordinated with the Terms of Use, Privacy Policy, Acceptable Use Policy and, where contracted, the Order, Business Agreement, DPA and SLA. The free evaluation follows the 7-day agreement and does not automatically receive commercial production targets.

External documents only form part of the relationship if they are made available to the CUSTOMER before acceptance and identified by title, version and date. Future policies will not be automatically incorporated, and no revision will retroactively amend a contract; contractual changes require a written amendment accepted by the parties, subject to mandatory rules.

Identification of the provider

The PROVIDER is COREPTT TECNOLOGIA LTDA, trading as COREPTT TECNOLOGIA, registered with the 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.

Sales and contracting: sales@coreptt.com. Registered telephone: (11) 9839-0601. Legal matters, privacy, integrity and security: legal@coreptt.com.

The PROVIDER is the legal entity responsible for the commitments it undertakes in the corePTT instruments. The CUSTOMER and representatives of both parties will be identified in the applicable instrument, with authority to approve the scope and sign.

1 Scope and transparency

This document describes the expected security model for the corePTT offering. It must not be interpreted as a certificate, audit report or guarantee that no incidents will occur. The published version must correspond to the controls actually implemented and the evidence that the PROVIDER can present under confidentiality.

2 Shared responsibility

Responsible party	Main obligations
PROVIDER	protect components under its administration, manage internal access, respond to incidents and supervise suppliers
CUSTOMER	define users, groups, permissions, retention, authorized devices and internal recording and location tracking rules
User	protect credentials and the device, install updates, follow guidance and report suspicions
Telecommunications operator and suppliers	meet their network, infrastructure, product, support and security obligations under their own contract

3 Governance

The PROVIDER must maintain designated persons responsible for security, privacy, operations and incident response; an inventory of relevant assets; periodic risk assessments; supplier acceptance criteria; change rules; and records that demonstrate the decisions taken. Exceptions must have an owner, justification, time limit and compensating control.

4 Identity and access

Administrative accounts must be individual, granted with the least privilege necessary and reviewed periodically. Multifactor authentication must be required for administrative functions whenever the component supports the feature. Credentials, keys and secrets must not be stored in plaintext or shared through inappropriate channels.

5 Environments and changes

Development, test and production environments must be separated according to the architecture. Real personal data must not be used in testing unless there is a documented need and equivalent protection. Relevant changes must have a request, assessment, approval, test, rollback plan and record appropriate to the risk.

6 Protection of data in transit and storage

The Technical Annex must identify transport protocols, available encryption, key management, storage regions and exceptions. The PROVIDER does not claim end-to-end encryption when servers need to process, record, transcode or distribute communications. The CUSTOMER will receive a sufficient description to understand this design before enabling recordings or high-risk data.

7 Records and monitoring

Administrative events, authentications, permission changes and critical actions must generate records proportionate to the risk. Access to logs is restricted, and their retention follows the security purpose, the Marco Civil da Internet, the DPA and the Service Order. Monitoring does not authorize indiscriminate surveillance of workers or content.

8 Vulnerabilities and updates

The PROVIDER must monitor vulnerabilities affecting components under its management, prioritize fixes according to criticality and exploitation risk, and maintain a process for emergency updates. Unsupported components must be replaced, isolated or protected by a documented compensating control.

9 Development and integrations

Software changes must undergo an appropriate review, dependency control and testing. APIs must require authentication, restrict scope and apply limits against abuse. Integrations supplied by the CUSTOMER must be assessed before receiving access to high-impact data or functions.

10 Backups and continuity

Backup frequency, retention period, region, restoration tests, recovery point objective and recovery time objective must be stated in the Technical Annex when they constitute contractual commitments. A backup is not a permanent archive and does not replace export by the CUSTOMER.

11 Suppliers

Suppliers with access to data or infrastructure must be assessed according to criticality and undertake confidentiality, security, incident, deletion and cooperation obligations. The PROVIDER must maintain the list of subprocessors and verify that international transfers have a valid mechanism.

12 People and confidentiality

Employees and service providers with access must be bound by a duty of confidentiality, receive guidance appropriate to their role and lose access when the need ends. Exceptional support access must be authorized, limited in time and recorded whenever the architecture permits.

13 Incident response

The process will include receipt of the alert, classification, preservation of evidence, containment, eradication, recovery, impact analysis and lessons learned. The PROVIDER, as processor of the CUSTOMER's data, will notify the controller of identified incidents without undue delay, with the available information and updates, without waiting for the investigation to end. The controller will assess and make notifications to the ANPD and data subjects when required, within the statutory periods. Each party retains its own obligations. Records of incidents involving personal data will follow the statutory retention period, including five years where applicable, in accordance with the LGPD and Resolution CD ANPD No. 15 of 2024.

14 Evidence and audits

Upon reasonable request and a confidentiality undertaking, the PROVIDER may supply completed questionnaires, architecture descriptions, policies, test reports or other available evidence. Delivery must protect trade secrets, other customers' security and information that increases the risk of attack.

15 Certifications and statements

ISO certifications, audit reports, approvals and technical compliance, including 3GPP standards, may only be advertised or contracted with valid evidence, a defined scope and a current validity period. This document does not claim certification or an independent audit. Functional compatibility and product development are not equivalent to certification.

16 Assets media and disposal

Assets that store or process information must have an owner, classification and lifecycle appropriate to the risk. Return, reuse, sale or disposal of equipment or media must include secure data removal, verification of the result and a record when criticality warrants it. The CUSTOMER's devices remain subject to its internal rules.

17 Physical infrastructure and providers

Physical controls of data centers, telecommunications and third-party facilities follow the responsibility and evidence of the respective provider. The PROVIDER must assess these controls according to criticality and must not advertise a location, redundancy, certification or surveillance that it cannot demonstrate. Facilities under direct management must restrict and record access in a manner appropriate to the risk.

18 Resilience tests

Continuity, backup restoration and incident response plans must be exercised at intervals proportionate to the risk. Results, gaps and persons responsible for corrections must be recorded. RTO, RPO, alternative region and test frequency only constitute a contractual commitment when stated in the Order or Technical Annex.

19 Review and indicators

The PROVIDER must review this document and the set of controls following a relevant change, a material incident or, at a minimum, within an internally defined periodic cycle. The analysis may consider privileged access, vulnerabilities, restorations, suppliers, incidents, exceptions and remediation plans, without disclosing information that increases the risk of attack.

20 Security contact

Security alerts and responsible vulnerability reports may be sent to legal@coreptt.com. Information about ongoing incidents must be treated confidentially to avoid compromising containment, investigation or third parties.

Supplier chain security

The PROVIDER assesses relevant infrastructure, software, API and equipment dependencies according to risk and the contracted scope. Changes of supplier or subprocessor that affect security, privacy or continuity must follow the contractual process and the DPA.

The Security and Trust page describes practices and controls, but must not claim certification, an independent audit or full compliance with a standard that has not been formally obtained and maintained.

Segregation in shared infrastructure

Shared environments must adopt logical segregation of accounts, profiles, data and permissions compatible with the validated architecture. Computing, storage, network and support service resources

may be shared by multiple CUSTOMERS. Controls and tests will be proportionate to the risk; no claim of physical isolation will be made without a specific contract and evidence.

Dedicated environments and server management

In a dedicated environment, the PROVIDER manages the resources expressly reserved for the CUSTOMER, within the contracted layer. This may cover provisioning, secure configuration, updates, monitoring, capacity, administrative accounts, technical logging, backup, recovery and incident response. Excluded or jointly managed items must be stated in the Service Order.

The PROVIDER's responsibility for administering the environment does not turn third-party physical infrastructure, cloud services, connectivity or licensed software into its own resources. The PROVIDER is responsible for the selection, configuration and management it undertakes; the external provider is responsible for its layer; and the CUSTOMER is responsible for users, data, terminals and decisions under its control.

Backup and recovery

Frequency, retention, scope, encryption, location, restoration tests, RPO and RTO only constitute a commitment when recorded in the accepted plan or Order. Backup is a recovery control and does not replace a historical archive. The free 7-day evaluation does not include a backup or recovery guarantee, unless an obligation has been expressly accepted before activation; proportionate security measures and legal duties remain enforceable.

In the free trial, the CUSTOMER must perform or request the necessary exports before the trial ends. Without a contract or legally necessary preservation, operational content will be deleted or anonymized within 30 calendar days after the end of the trial; any residual backup copies will be purged within 90 days after the end of the trial, with restricted access and no operational reuse. The periods will be validated against the architecture before signature. Statutory retention and the lawful exercise of rights follow their own periods and purposes. The trial does not guarantee retention of recordings for 90 days or recovery of content already deleted.

Document control

Field	Record
Entity responsible for the document	COREPTT TECNOLOGIA LTDA
Coordination and legal review	Responsible person to be appointed by the PROVIDER before signature
Sales and contracting	sales@coreptt.com
Legal matters privacy and integrity	legal@coreptt.com
Revision and date	1.3 • 14 October 2026
Status	Draft for legal review