



Push-to-talk solution

CORPORATE AND CONTRACTUAL DOCUMENTATION

corePTT Acceptable Use Policy

Permitted conduct restrictions and response to misuse

corePTT platform

Compliance and governance
Security and data protection

05

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 Acceptable Use Policy

Permitted conduct restrictions and response to misuse

Legal and commercial entity	COREPTT TECNOLOGIA LTDA
CNPJ	69.599.966/0001-93
Trade name	COREPTT TECNOLOGIA
Registered address	Rua Comendador Torlogo Dauntre, nº 74, sala 1207, Cambuí, Campinas/SP, CEP 13025-270
Municipality and state	Campinas/SP
Postal code	13025-270
Brand and platform	corePTT
Revision	1.3
Revision date	14 October 2026
Document status	Draft for legal review

This Policy establishes practical rules for communication, recording, location tracking, APIs, devices and security. It applies to contracted operations and the free 7-day evaluation, subject to the features, limits, purposes and responsibilities documented in each instrument.

This document forms part of the corePTT documentation set and must be read together with the instruments applicable to its purpose. For the free trial, the 7-Day Trial Agreement and the activation schedule apply. For paid operations, the documents identified in the Service Order apply. Incorporation requires that the document be made available before acceptance, with its title, revision and date; future amendments have no automatic or retroactive contractual effect.

Identification of the PROVIDER

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, hereinafter the PROVIDER.

The brand used is corePTT, with core in lowercase letters and PTT in uppercase letters. The PROVIDER must be identified in the commercial, tax and evaluation instruments; the brand does not replace identification of the legal entity.

Sales and contracting: sales@coreptt.com; registered telephone: (11) 9839-0601. Legal matters, privacy and integrity: legal@coreptt.com. Revision 1.3 dated 14 October 2026. Draft for legal review.

1 Purpose

This Policy protects people, networks, devices, customers and the platform itself. It applies to users, administrators, integrations, APIs, connected applications and anyone who uses a corePTT credential or resource.

2 Authorized use

The service must be used for legitimate professional communication, within the scope approved by the CUSTOMER and the permissions assigned. Users may not bypass controls, exploit a function for an undisclosed purpose or use another organization's environment without authorization.

3 Prohibited content and conduct

- threats, stalking, harassment, discrimination, exploitation, extortion or incitement to violence;
- unlawful, fraudulent or defamatory material, or material that violates confidentiality, image rights, intellectual property or privacy;
- use to coordinate crime, obstruct authorities or conceal illegal activity;
- recording, filming or locating a person without a legal basis and adequate information;
- disclosure of credentials, personal data or confidential information beyond operational need;
- deliberately false communication that may compromise security, continuity or incident response.

4 Security and integrity

- do not conduct load, penetration or security tests, scanning, traffic interception, vulnerability exploitation or attempts to access other environments without specific written authorization;
- do not introduce malware, destructive code, abusive automation or persistence mechanisms;
- do not bypass authentication, limits, audit logging, license restrictions or administrative controls;
- do not use a generic account when the environment requires individual traceability;
- do not connect a compromised device, a device with its protections removed or an unsupported version when this increases risk.

5 Use of APIs and integrations

Integrations must comply with the documentation, call limits, credential scope and authorized environment. Extraction without a legitimate purpose and authorization, reidentification of anonymized data, unauthorized replication or resale of the service and copies without compatible controls are prohibited. Keys and secrets must be protected and replaced if exposed; APIs not enabled within the scope are outside the trial.

6 Privacy and monitoring

The CUSTOMER must configure recording and location tracking proportionately to the stated purpose. Using corePTT for covert surveillance, discriminatory profiling, control of private life or exclusively automated decision-making without the safeguards required by law is prohibited. Access to operational content must follow functional need and audit logging requirements.

7 Use in critical environments

Users must maintain alternative means and must not rely exclusively on corePTT for assistance or command whose failure could cause death, serious injury, environmental harm or significant material loss. Any commercial commitment for critical use requires a specific project, tests, redundancy, contingency planning and formal acceptance supported by technical evidence. In the free trial, use as an emergency system or mission-critical infrastructure is outside the scope. The platform does not replace public emergency services.

8 Network resources

Causing disproportionate load, unauthorized automated calls, mass transmissions, interference, identity fraud, source masking or use that degrades other customers' experience is prohibited. The PROVIDER may apply reasonable technical limits to preserve security and availability.

9 Equipment and serial numbers

Devices supplied under rental or loan-for-use arrangements must be used at the agreed location, for the agreed purpose and in the agreed configuration. The CUSTOMER may not remove asset identification, alter firmware without authorization, break a seal or transfer equipment to a third party outside the contract.

10 Responsible vulnerability reporting

Suspected vulnerabilities must be reported confidentially to legal@coreptt.com, with a description, minimized evidence and a secure contact method. Reporting does not authorize access to third-party data, persistence, disruption or invasive testing, nor does it create an automatic reward. Any tests require written authorization specifying scope, time window and responsibilities; disclosure must respect rights, confidentiality and security.

11 Investigation

The PROVIDER may preserve relevant records, limit access and request information necessary to investigate a violation. It will consider severity, recurrence, impact and cooperation, and restrict measures to what is necessary. Processing evidence must comply with purpose, legal basis, restricted access and a justified retention period, without authorizing indiscriminate surveillance of content.

12 Consequences

A violation may result in guidance, blocking, replacement of credentials, suspension or termination, depending on severity, risk, law and the contract. The PROVIDER will state the reason where permitted and offer an opportunity to correct the situation where compatible with the risk. Urgent measures may be immediate. Communications to authorities or third parties require a legal basis and proportionate scope; the free nature of the service does not remove duties of good faith, security and data protection.

13 CUSTOMER responsibility

The CUSTOMER must train users, keep administrators up to date, review access, disable accounts of people who are no longer affiliated and investigate misuse under its control. It must cooperate with the PROVIDER in containing incidents and must not instruct users to violate this Policy.

14 Questions and exceptions

Operational exceptions require written approval from the PROVIDER and the CUSTOMER's authorized representative, specifying scope, period, risks and controls. They may not authorize unlawful conduct or waive mandatory rules. Failure to respond does not mean authorization. Changes to features and trial duration must be recorded, and contacting sales does not extend access.

Third-party rights and authorized integrations

Users may not bypass licenses, copy software, use a trademark or logo without authorization, extract code, manipulate firmware, create unapproved integrations or violate the terms of manufacturers and suppliers connected to the environment.

Use of evaluation environments

The standard trial lasts 7 calendar days, equivalent to 168 hours from the notified activation, with a license fee of R\$ 0,00 and a scope validated in the activation schedule. It does not include a commercial SLA or continuous availability. Use for emergencies, critical production, unlawful surveillance, processing outside the authorized purpose or circumvention of licenses, security and contracting procedures is prohibited. Sensitive data and data relating to children or adolescents are excluded, unless there is a prior specific agreement and the legal requirements are met.

The CUSTOMER must favor fictitious, anonymized or minimized data and arrange its exports before the trial ends. There is no automatic renewal or automatic conversion to a paid service, purchase obligation or retroactive charge for the free license. To continue, the CUSTOMER must formalize a contract through sales@coreptt.com; registered telephone: (11) 9839-0601. Without a contract or lawful preservation, operational content will be deleted or anonymized within 30 days after the end of the trial and residual backups will be purged within 90 days after the end of the trial, without operational reuse; these periods are subject to validation of the architecture before signature. The trial does not guarantee restoration or recordings for 90 days.

Public bodies and companies must internally authorize the trial, appoint a responsible person and permit only data compatible with the purpose and information classification. The parties will comply with applicable integrity and anti-corruption legislation, without undue advantage, fraud or unlawful favoritism. Approvals, scope changes and extensions will be documented. Reports of irregularities may be sent to legal@coreptt.com, with a restricted investigation and a prohibition on retaliation for good-faith conduct.

This revision and the other policies will only form part of the agreement if they are made available before acceptance and identified by title, version and date. New versions will not be automatically incorporated or retroactively amend obligations. This Policy does not assert certifications, audits or technical compliance that have not been demonstrated.

Document control

Field	Record
Entity responsible for documentation	COREPTT TECNOLOGIA LTDA
Document status	Draft for legal review
Sales channel	sales@coreptt.com
Legal matters privacy and integrity	legal@coreptt.com