CODENEX SRLS
Operating office: Via Duca della Verdura 27 - 90143 Palermo (PA)
Registered office: Via Resuttana 360 - 90146 Palermo (PA)
VAT IT07425080822 - CF 07425080822 - REA PA-457974
PEC: codenex@pecsicura.com - SDI 9SUB64Q
E-mail: hello@codenex.it - Sales: +39 02 40042 262

ANTI-FRAUD AND ACCEPTABLE USE POLICY (AUP)

Protection of accounts, traffic, numbers and infrastructure

CODENEX SRLS - CloudVoce.it | **Version:** 1.8 - 31 October 2026

1. Purpose and scope

This policy applies to accounts, devices, lines, API, webhooks, WebRTC and tenant traffic. It aims to prevent unauthorised access, fraud, spoofing, artificial traffic, compromise and harm to other customers or networks.

2. Prohibited uses

- vishing, phishing, voice spam, robocalls or campaigns without legal requirements;
- caller-ID alteration, unauthorised numbers or impersonation;
- artificial traffic, revenue-share abuse or abusive calls to high-cost destinations;
- SIP scanning, attacks, unauthorised access, interception or compromise;
- harassment, threats, unlawful content, secrecy breaches or circumvention of blocks;
- resale, credential sharing or safety-critical use without written agreement.

3. Customer security duties

- unique passwords, administrator 2FA where available and least-privilege roles;
- protection of API tokens, SIP credentials and devices;
- updates for phones, browsers, routers and firewalls;
- regular review of calls, extensions, trunks and alerts;
- immediate compromise reporting and credential rotation;
- destination, prefix and concurrency limits appropriate to use.

4. Technical controls

CloudVoce uses documented controls such as rate limits, fail2ban, SIP guard, progressive blocks, authentication and concurrent-call monitoring and risky-destination controls. No infallible or fully autonomous fraud-prevention system is represented. The Customer remains responsible for use and costs generated through its credentials, subject to supplier or carrier liability under law and contract.

5. Measures where risk arises

CODENEX may restrict calls, prefixes, APIs, extensions or trunks; require credential changes; isolate the tenant; temporarily suspend telephony; preserve evidence; and cooperate with carriers or authorities. Action may be immediate where delay increases risk.

6. Notice, review and restoration

Where consistent with investigation and security, CODENEX informs the contact. The Customer may request review by ticket with verifiable evidence. Restoration requires removal of the cause, credential rotation, device checks and, where needed, payment or identity verification.

7. Reporting

Abuse and incidents should be reported through the panel or to hello@codenex.it without passwords. Urgent reports should include tenant, time, affected numbers and a safe contact.