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

POLICY ANTIFRODE E USO ACCETTABILE (AUP)

Protezione di account, traffico, numerazioni e infrastruttura

CODENEX SRLS - CloudVoce.it | **Versione:** 1.8 - 31 ottobre 2026

1. Finalita' e ambito

La policy si applica ad account, telefoni, linee, API, webhook, WebRTC e traffico gestito dal tenant. Mira a prevenire accessi abusivi, frodi, spoofing, traffico artificiale, compromissioni e danni ad altri clienti o reti.

2. Usi vietati

- vishing, phishing, spam vocale, robocall o campagne prive dei requisiti di legge;
- alterazione del CLI, uso di numeri non assegnati o impersonificazione;
- traffico artificiale, revenue share abuse, chiamate abusive a numeri speciali o destinazioni ad alto costo;
- scansioni SIP, attacchi, tentativi di accesso, intercettazione o compromissione di account e terzi;
- molestie, minacce, contenuti illeciti, violazione del segreto delle comunicazioni o elusione di blocchi;
- rivendita, condivisione di credenziali o uso safety-critical senza accordo scritto.

3. Obblighi di sicurezza del Cliente

- password uniche, 2FA per gli amministratori ove disponibile e ruoli minimi;
- protezione di token API, credenziali SIP e dispositivi;
- aggiornamento di telefoni, browser, router e firewall;
- verifica periodica di chiamate, interni, trunk e notifiche;
- segnalazione immediata di compromissioni e revoca delle credenziali esposte;
- configurazione di prefissi consentiti, limiti e numeri bloccati coerenti con l'uso.

4. Controlli tecnici

CloudVoce usa regole e soglie documentate: rate limit, fail2ban, SIP guard, blocchi progressivi, controllo di autenticazioni, chiamate contemporanee e destinazioni a rischio. Non viene dichiarato un sistema infallibile o un algoritmo autonomo capace di impedire ogni frode.

Il Cliente resta responsabile dei costi e degli usi generati dalle proprie credenziali, salvo responsabilita' imputabile a CODENEX o all'operatore secondo legge e contratto.

5. Misure in caso di rischio

CODENEX puo' limitare chiamate, prefissi, API, interni o trunk; forzare il cambio credenziali; isolare il tenant; sospendere temporaneamente la telefonia; conservare evidenze e collaborare con operatori o autorita'. La misura puo' essere immediata quando il ritardo aumenta il rischio.

6. Comunicazione, verifica e ripristino

Quando non compromette indagini o sicurezza, CODENEX informa il referente. Il Cliente puo' chiedere revisione tramite ticket, fornendo elementi verificabili. Il ripristino richiede rimozione della causa, rotazione delle credenziali, controllo dei dispositivi e, se necessario, verifica del pagamento o dell'identita'.

7. Segnalazioni

Abusi e incidenti vanno segnalati dal pannello o a hello@codenex.it senza inviare password. Per urgenze indicare tenant, orario, numeri coinvolti e un recapito sicuro.