

Robocall Mitigation Plan (RMD)

Kloud9 IT, Inc.

Legal Entity Name: Kloud9 IT, Inc.

Primary Business Address: 3465 S. Arlington Rd., Suite E #161, Akron, OH 44312

FCC Registration Number (FRN): 0038109104

Operating Company Number (OCN): N/A

Primary Robocall Mitigation / Compliance Contact:

Trent Milliron, CEO

Email: partners@kloudtel.com

Phone: 833-556-8383 x 800

Effective Date: March 4, 2026

Last Review Date: March 4, 2026

Next Scheduled Review Date: March 4, 2027

Record Retention Period: 2 years

1) Provider Role, Business Model, and Scope

Kloud9 IT, Inc. ("Kloud9") provides interconnected voice service to end users as a reseller. Kloud9 does not own or operate the underlying voice network elements used to originate calls, interconnect to the PSTN, or perform STIR/SHAKEN signing/authentication.

Kloud9 relies on one or more upstream wholesale providers ("Wholesale Provider") that fully control the network infrastructure and are responsible for technical STIR/SHAKEN implementation and network-level technical controls.

RMD Role Identification (for the submission form): Kloud9 is a "voice service provider without a STIR/SHAKEN implementation obligation" because Kloud9 lacks control over the network infrastructure necessary to implement STIR/SHAKEN.

2) STIR/SHAKEN Status and Explanation (Reseller / No Control)

Kloud9 does not implement STIR/SHAKEN directly due to lack of control over the network infrastructure necessary to do so. Kloud9's Wholesale Provider controls the signing/authentication and related network functions.

For RMD certification purposes, where asked to identify an applicable basis for no implementation, Kloud9 will state:

- "Unable to implement STIR/SHAKEN due to lack of control over the network infrastructure necessary to implement STIR/SHAKEN."

3) Robocall Mitigation Program Overview

Kloud9 maintains an appropriate robocall mitigation program designed for a reseller environment and focused on reducing the origination of illegal robocall traffic through:

- Know-Your-Customer (KYC) and due diligence for new and renewing customers;
- Contractual and policy controls prohibiting illegal robocalls/spoofing;
- Rapid investigation and escalation to the Wholesale Provider for network-level controls; and
- Traceback responsiveness and cooperation.

4) Know-Your-Customer (KYC) and Due Diligence Controls

Kloud9 takes affirmative measures to know its customers and apply due diligence to reduce the likelihood its services are used to originate illegal traffic.

4.1 Pre-Activation Identity Verification (New Customers)

For each new customer, Kloud9 collects and verifies, as applicable:

- Legal business name / DBA and business address
- Authorized user / signer identification and title/role
- Billing identity and payment method validation
- Email/phone validation for operational contacts
- Service use-case description (business purpose)
- Expected calling behavior (approx. volume patterns, geographic targets, and call type)
- Caller ID / number usage expectations (where relevant)

4.2 Risk-Based Screening and Red Flags

Kloud9 applies enhanced screening and/or may delay activation or require additional documentation when risk indicators appear, including:

- Unusually high call volume requested immediately upon activation
- Inconsistent or unverifiable business identity information
- Use-cases commonly associated with high fraud risk (e.g., impersonation-heavy verticals)
- Refusal to provide reasonable business identity documentation

4.3 Ongoing / Renewing Customer Review

Kloud9 periodically reviews customer accounts based on risk tier and/or triggering events (complaints, unusual activity notices, etc.). Reviews may include:

- Revalidation of key identity/contact information

- Review of complaint history and enforcement history
- Confirmation the customer's actual usage remains consistent with the stated use-case

5) Customer Contractual Controls and Acceptable Use Restrictions

Kloud9's customer agreements and acceptable use policies prohibit:

- Illegal robocalls and unlawful telemarketing practices
- Spoofing or transmitting misleading/invalid caller ID information
- Fraudulent calling campaigns
- Use of service to facilitate illegal traffic

Kloud9 reserves the right to take prompt action for suspected abuse, including suspension, termination, and coordination with Wholesale Provider network controls, consistent with its mitigation obligations.

6) Monitoring, Complaints Handling, and Enforcement

6.1 Alert Sources

Kloud9 investigates potential illegal calling activity based on:

- Consumer or enterprise complaints submitted to Kloud9
- Notices or escalations received from the Wholesale Provider
- Traceback requests or requests from the FCC, law enforcement, or the industry traceback consortium
- Any usage anomaly notifications available to Kloud9 through Wholesale Provider reporting

6.2 Investigation Workflow

Upon receipt of an alert, Kloud9 will:

- 1. Open an internal incident record and log date/time/source**
- 2. Identify related customer account(s), assigned numbers, and provisioning history**
- 3. Request supporting call-path detail and analytics from Wholesale Provider (as Kloud9 is a reseller)**
- 4. Contact the customer for explanation and, where relevant, documentation (e.g., proof of consent)**
- 5. Determine mitigation/enforcement actions and document results**

6.3 Enforcement Actions

Depending on severity and evidence, Kloud9 may:

- Issue warnings and require corrective actions
- Temporarily suspend outbound calling capability
- Request Wholesale Provider to apply network-level mitigation (blocking, rate-limits, other controls)
- Terminate service for confirmed or repeated illegal activity
- Preserve evidence and cooperate with traceback/law enforcement

7) Reliance on Wholesale Provider for Analytics and Technical Controls

Kloud9 does not operate network-level STIR/SHAKEN infrastructure or analytics systems directly. Kloud9 relies on Wholesale Provider for:

- Network-level call signing/authentication (STIR/SHAKEN where applicable)
- Call traffic analytics, abnormal pattern detection, and related technical controls
- Network-level mitigation actions (blocking, call rejection, rate limiting), as needed

Kloud9 will use Wholesale Provider-provided analytics and technical controls to inform investigations and mitigation steps, and will coordinate promptly with Wholesale Provider when network actions are needed.

8) Traceback Response Commitment (24 Hours) and Cooperation

Kloud9 commits to respond to all traceback requests from the FCC, law enforcement, and the industry traceback consortium within 24 hours and to cooperate fully in investigating and stopping illegal robocallers.

8.1 Traceback Intake and Escalation

Kloud9 maintains a designated compliance contact for traceback issues:

- Trent Milliron, CEO – partners@kloudtel.com – 833-556-8383 x 800

When a traceback request is received, Kloud9 will:

- Acknowledge receipt promptly
- Identify related customer account(s), numbers, and provisioning history
- Escalate to Wholesale Provider immediately for call-path logs and network data Kloud9 does not control
- Provide responsive information to the requesting entity within the required timeframe

8.2 Information Kloud9 Can Provide

As a reseller, Kloud9 can provide (as applicable):

- Customer identity/KYC and account records
- Assigned numbers/services and activation dates
- Billing/contact records and service history

- Incident/enforcement actions taken (suspension/termination/mitigation requests)
- Coordination details with Wholesale Provider regarding network-level mitigations

9) Upstream (Wholesale Provider) Diligence and Coordination

Kloud9 maintains:

- Current upstream Wholesale Provider business identity and escalation contacts (NOC/abuse/security)
- Procedures to promptly engage Wholesale Provider for investigation/mitigation when illegal activity is suspected
- Documentation of Wholesale Provider coordination for investigations, mitigation actions, and traceback responses

10) Recordkeeping and Retention (2 Years)

Kloud9 retains records for 2 years to support compliance, investigations, and traceback responsiveness, including:

- Customer onboarding and KYC documentation
- Customer agreements/AUP acceptance and key communications
- Complaint and incident records, investigations, and outcomes
- Traceback requests and responses
- Escalations and mitigation coordination with Wholesale Provider

11) Plan Maintenance, Updates, and Annual Review

Kloud9 reviews this plan at least annually and upon material changes (e.g., changes in upstream Wholesale Provider relationships, product changes, or significant compliance events). Kloud9 will update its RMD filing as required when information changes and will complete annual recertification obligations according to applicable FCC requirements.

Appendix A (Optional) – Wholesale Provider Details (Placeholder)

Wholesale Provider: [Placeholder – maintained internally]

Abuse/NOC/Security Contacts: [Placeholder]

Services Provided: PSTN interconnection, call origination/termination, STIR/SHAKEN implementation, analytics, network-level mitigation

If Wholesale Provider identification is treated as sensitive, Kloud9 may provide a redacted plan for public posting and maintain an unredacted version internally and/or submit confidential materials following FCC procedures, as applicable.