Robocall Mitigation Plan

Korha Tech, LLC | Draft for review | November 17, 2026

DRAFT - NOT READY FOR FCC FILING
This is a proposed plan. Korha Tech must confirm that the procedures described are actually in place, complete the bracketed details, and review the plan for accuracy before submitting it.

1. Company and program contact

Legal name: Korha Tech, LLC
Address: 14706 Canal Crossing Blvd, Gulfport, MS 39503-5452
CEO: Kianna Hayes
Email: korina@korha.tech **Phone:** 929-577-6974
EIN: 41-3453622 **FRN:** 0039239686

Designated robocall mitigation contact: [Confirm name, title, phone, email and 24-hour availability.]
Services and call-chain roles: [Describe services and identify whether the company originates or terminates calls, acts as a gateway or non-gateway intermediate provider, or serves more than one role. Describe any foreign-originated traffic.]

2. Purpose and oversight

This proposed program is designed to prevent illegal robocalls and caller ID spoofing from being originated, carried or processed through the company's services, as applicable to its role. The designated compliance officer oversees customer due diligence, monitoring, investigations, traceback response and program review. [Identify the person responsible and the review schedule.]

3. Customer verification and renewal

Before service activation, verify each customer's legal identity, business address, authorized representatives and ownership or control using reliable records. Review intended use, call sources and destinations, estimated volumes, calling practices, number ownership or authorization, and relevant consent and opt-out procedures. Resolve discrepancies before activation. Review scripts or recorded material when appropriate.

Use contracts that prohibit illegal robocalls and spoofing, require cooperation with investigations and tracebacks, and allow corrective action, suspension or termination. Reassess customer information and use at renewal and when traffic patterns or other risk indicators change. [Specify the checks and review frequency actually used.]

4. Upstream provider due diligence

Identify each upstream provider and its business, operational and compliance contacts; document the services it supplies and expected traffic sources. Review relevant FCC registrations and Robocall Mitigation Database entries, investigate discrepancies, and document decisions before accepting traffic. Reassess providers after complaints, tracebacks, unusual calling patterns or material changes. [Identify actual verification sources, review schedule and responsible personnel.]

5. Traffic monitoring and analytics

Review call-detail records and relevant network alerts for unusual volume or bursts, repeated short calls, rapid caller ID changes, invalid or unauthorized numbers, unusual completion patterns and complaints. Investigate alerts against the customer's expected traffic and the facts of the calls; no single indicator alone establishes that traffic is illegal.

Actual analytics systems: [Identify the systems and any third-party vendors used, or accurately state that no analytics system is used. Describe data reviewed, alert criteria, review frequency, responsible personnel and how alerts are investigated.]

6. Investigation and corrective action

Log complaints, tracebacks and monitoring alerts. Preserve relevant records, identify the customer or upstream source, request supporting information and assess the facts. Where warranted, restrict or block affected traffic, suspend service, require remediation or terminate the relationship. Record the outcome, explain actions to affected customers as required, and review potential false positives in accordance with applicable rules.

7. Tracebacks and 24-hour response

Maintain a documented process to respond fully within 24 hours to traceback requests from the FCC, law enforcement and the registered industry traceback consortium, as applicable. Record the receipt time, identify the relevant calls and their immediate upstream and downstream parties, preserve records, supply responsive information, and document follow-up and remediation. [Confirm the company's 24-hour commitment and identify its contact, staffing and escalation process.]

8. STIR/SHAKEN status and any exemption

[State whether STIR/SHAKEN is fully, partially or not implemented, and explain the status for each applicable role and network segment. Identify the signing and verification arrangements and the company's SPC token and certificate status where applicable.]

[If claiming an exemption or extension, identify the applicable rule or FCC order and explain the company-specific facts, affected services and network segments. Do not claim an exemption based solely on the company's size or on another company's circumstances.] The FCC has recognized an exemption for providers that lack control over the network infrastructure necessary to implement STIR/SHAKEN: First Caller ID Authentication Report and Order, FCC 20-42, paragraph 40. An implementation exemption does not remove applicable robocall mitigation or filing obligations.

9. Records, training and review

Retain customer and upstream due-diligence records, call-detail data, monitoring alerts, complaints, traceback responses and corrective actions in accordance with applicable requirements and the company's actual retention policy. Restrict access to authorized staff and protect sensitive information. Train relevant personnel and periodically review the program. [Specify retention periods, training frequency and responsible personnel.]

10. Approval and filing review

Before submitting, replace all bracketed text; verify that the listed controls are implemented; confirm the contact, call-chain roles, STIR/SHAKEN status and any exemption; and independently review the RMD certification questions, including applicable enforcement history. An authorized officer should review and approve the completed plan and maintain the filing as required.

Authorized officer: Kianna Hayes, CEO **Approval date:** _____

FCC reference materials

FCC discussion of RMD plan requirements: https://docs.fcc.gov/public/attachments/DA-26-872A1.pdf
FCC guidance on implementation and exemptions: https://docs.fcc.gov/public/attachments/DA-26-72A1.pdf
FCC discussion of the infrastructure exemption: https://docs.fcc.gov/public/attachments/FCC-24-120A1.pdf