

Robocall Mitigation Plan

Provider Type: Managed Service Provider (MSP) / VoIP Service Provider

Organization Name: IT Architech Inc.

FCC Registration Number (FRN): 0037934221

1. Purpose

This Robocall Mitigation Plan (“Plan”) describes the specific actions and controls implemented by **IT Architech Inc.** to prevent the origination, transmission, and facilitation of illegal robocalls on our network, in accordance with **47 CFR §64.6305**, FCC robocall mitigation rules, and associated guidance for inclusion in the **FCC Robocall Mitigation Database (RMD)**.

2. Scope of Services

IT Architech Inc. operates as a **Managed Service Provider (MSP) and interconnected VoIP provider**, delivering hosted voice services to business customers. This Plan applies to:

- All outbound calls originated by customers
 - All inbound and transmitting voice traffic on our network
 - All DID numbers, SIP trunks, softphones, PBX systems, and related VoIP services
-

3. Regulatory Compliance Statement

IT Architech Inc. certifies that it has implemented reasonable and effective measures to mitigate the risk of illegal robocalls and complies with applicable laws and regulations, including but not limited to:

- Telephone Consumer Protection Act (TCPA)
 - FCC robocall mitigation and caller ID authentication rules
 - STIR/SHAKEN requirements
 - Truth in Caller ID Act
 - Applicable state and federal telemarketing laws
-

4. Customer Due Diligence and Onboarding Controls

4.1 Know Your Customer (KYC)

Prior to provisioning outbound calling capabilities, IT Architech Inc. performs customer vetting that may include:

- Verification of legal business name and address
- Collection of tax ID, business registration, or equivalent documentation
- Verification of authorized contacts and billing ownership
- Review of customer website and business purpose

4.2 Use Case Validation

Customers must disclose intended outbound calling use cases. Use cases such as:

- Telemarketing
 - Political calling
 - Debt collection
 - Automated or high-volume dialing are classified as **higher-risk** and subject to enhanced scrutiny, additional documentation, and ongoing monitoring.
-

5. Acceptable Use Policy Enforcement

All customers must agree to an **Acceptable Use Policy (AUP)** that expressly prohibits:

- Illegal robocalls or autodialed calls without proper consent
- Spoofing caller ID with intent to defraud or mislead
- Transmission of scam, phishing, or fraudulent calls
- Violations of TCPA, FCC rules, or applicable laws

Failure to comply may result in immediate suspension or termination of service.

6. STIR/SHAKEN Implementation

6.1 Outbound Call Authentication

IT Architechs Inc. has implemented STIR/SHAKEN authentication for outbound calls where technically feasible. We assign attestation levels as follows:

- **A (Full Attestation):** Customer identity and number ownership verified
- **B (Partial Attestation):** Customer authenticated but number ownership not fully verified
- **C (Gateway Attestation):** Traffic passing through our network without a direct customer relationship

6.2 Number Authorization

We verify customer authorization to use assigned DID's or numbers prior to enabling outbound calling.

7. Traffic Monitoring and Analytics

7.1 Continuous Monitoring

We monitor calling patterns for indicators of illegal robocalls, including:

- High-volume or burst dialing
- Short call durations
- Repeated calls to invalid, unassigned, or sequential numbers

- Abnormal answer-seizure ratios (ASR)
- Excessive failed or blocked call attempts

7.2 Automated Alerts and Review

Automated alerts are generated when thresholds are exceeded. Alerts are reviewed by trained personnel for investigation and response.

8. Mitigation Actions and Call Blocking

8.1 Proactive Mitigation

Upon detection of suspicious or unlawful activity, IT Architech Inc. may take immediate action, including:

- Throttling call rates
- Blocking specific numbers, routes, or traffic sources
- Temporarily suspending outbound calling
- Full service suspension pending investigation

8.2 Escalation and Enforcement

Confirmed violations may result in:

- Service termination
 - Permanent number blocking
 - Reporting to upstream carriers, regulators, or law enforcement
-

9. Complaint Handling and Traceback Cooperation

9.1 Complaint Intake

IT Architech Inc. maintains procedures to receive and track robocall complaints from:

- Consumers
- Upstream/downstream carriers
- Regulatory bodies

9.2 Traceback Cooperation

We respond promptly to legitimate traceback requests and cooperate with authorized traceback organizations, providing call detail records and customer information as permitted by law.

10. Employee Training

Relevant personnel receive periodic training covering:

- Robocall laws and FCC requirements
 - Fraud detection indicators
 - Internal escalation procedures
-

11. Recordkeeping and Review

We maintain records related to:

- Customer onboarding and verification
- Traffic monitoring and mitigation actions
- Complaints and enforcement actions

This Plan is reviewed periodically and updated as necessary.

12. FCC Robocall Mitigation Database Certification

IT Architech Inc. certifies that:

- It has implemented STIR/SHAKEN where required or feasible **OR**
 - It has implemented a robocall mitigation program consistent with FCC requirements
 - Information submitted to the FCC Robocall Mitigation Database is accurate and up to date
-

13. Contact Information

Robocall Mitigation Contact:

John J Wiecezak IV / Infrastructure Architech
IT Architech Inc.
FCC@itatsp.com
314-802-9766