



ORBITEL TELECOM

ROBOCALL MITIGATION PROGRAM

Submitted to the Federal Communications Commission
Robocall Mitigation Database

1. COMPANY OVERVIEW

Company Name: Orbitel Telecom

Role in Call Chain: Voice Service Provider, Gateway Provider, and Non-Gateway Intermediate Provider

Services Provided: Domestic and international voice telecommunications services

Orbitel Telecom operates as a comprehensive telecommunications provider serving business customers across the Brazilian market. We provide originating, terminating, and transit voice services through modern IP-based networks.

2. OBJECTIVES AND SCOPE

2.1 General Objective

Establish comprehensive guidelines and technical measures to prevent, identify, block, and effectively mitigate illegal automated phone calls (robocalls) across all portions of our network infrastructure.

2.2 Specific Objectives

- Ensure compliance with 47 CFR § 64.6305 robocall mitigation requirements
 - Implement STIR/SHAKEN call authentication where technically feasible
 - Protect network infrastructure from abuse and misuse leading to illegal robocalls
 - Provide transparency to regulatory agencies and customers regarding anti-fraud actions
 - Reduce the incidence of illegal automated calls on our network
 - Cooperate fully with law enforcement and regulatory investigations
-

3. NETWORK INFRASTRUCTURE AND STIR/SHAKEN IMPLEMENTATION

3.1 Network Architecture

Orbitel Telecom operates a network environment consisting of:

- Modern IP-based voice networks with SIP capabilities
- Interconnection facilities with major carriers and intermediate providers
- International capacity agreements for overseas traffic

3.2 STIR/SHAKEN Implementation Status

IP Network Portions: Orbitel is implementing STIR/SHAKEN call authentication on IP-enabled portions of our network, including:

- SIP-based customer connections
- IP-to-IP interconnections with STIR/SHAKEN-capable carriers

- Outbound call authentication for calls we originate
- Verification of inbound STIR/SHAKEN signatures where available

TDM Network Portions: Certain portions of our network rely on legacy TDM technology that cannot technically support STIR/SHAKEN implementation. For these network segments, Orbitel:

- Maintains participation in industry working groups developing non-IP authentication solutions
 - Implements alternative robocall mitigation measures detailed in this program
 - Plans for technology upgrades as economically feasible
-

4. CUSTOMER ONBOARDING AND VERIFICATION

4.1 Know Your Customer (KYC) Procedures

New Customer Registration:

- Require official documentation and identity verification for all new customers
- Perform cross-checking of customer data using public and private databases
- Require signed Terms of Service agreement explicitly prohibiting illegal robocalling
- Conduct credit checks and financial verification for business customers
- Validate business legitimacy for all commercial customers

Enhanced Due Diligence:

- Additional scrutiny for high-volume customers or those requesting unusual calling patterns
- Regular review of customer calling patterns and destinations
- Periodic re-verification of customer information and business status

4.2 Traffic Limitations for New Customers

- Implement initial call volume limits for new customers during probationary period
 - Monitor calling patterns, duration, and success rates during initial service period
 - Gradually increase limits as legitimate usage patterns are established
 - Maintain automated alerts for unusual traffic spikes or patterns
-

5. NETWORK MONITORING AND TRAFFIC ANALYSIS

5.1 Real-Time Monitoring Systems

Orbitel employs comprehensive network monitoring including:

- **Call Detail Record (CDR) Analysis:** Real-time analysis of calling patterns, including:
 - Call volume per customer and time period
 - Average call duration and completion rates
 - Destination analysis for unusual patterns
 - Sequential dialing pattern detection
- **Automated Alert Systems:** Configured to trigger on:
 - Abnormal call volume spikes (>X calls per minute threshold)
 - Short duration calls indicative of robocalling

- High-volume calls to invalid or disconnected numbers
- Calls exhibiting government impersonation patterns

5.2 Traffic Blocking and Mitigation

Immediate Response Capabilities:

- Real-time blocking of suspicious traffic pending investigation
- Do Not Originate (DNO) list implementation and maintenance
- Collaboration with Industry Traceback Group (ITG) for coordinated responses
- Integration with industry-shared blocked number databases

Call Screening and Validation:

- Implementation of calling party number validation where technically feasible
 - Blocking of obviously spoofed or invalid calling party numbers
 - Filtering of international traffic exhibiting domestic spoofing patterns
-

6. CUSTOMER EDUCATION AND CONTRACT TERMS

6.1 Acceptable Use Policies

All customer service agreements include:

- Express prohibition of illegal robocalling activities
- Requirements for valid calling party identification
- Obligations to comply with applicable telemarketing regulations
- Right of Orbitel to suspend service for policy violations

6.2 Customer Education Initiatives

- Provide clear information about illegal robocalling practices and consequences
 - Maintain customer support channels for reporting suspected abuse
 - Regular communications about regulatory requirements and best practices
 - Technical guidance for proper calling party number presentation
-

7. COOPERATION WITH LAW ENFORCEMENT AND INVESTIGATIONS

7.1 Traceback and Investigation Support

Orbitel commits to:

- Respond fully and promptly to all traceback requests from the FCC, law enforcement, and ITG
- Maintain detailed call records sufficient for effective traceback
- Provide technical assistance for investigation of illegal robocalling campaigns
- Cooperate with regulatory agencies in enforcement actions

7.2 Industry Collaboration

- Membership in relevant industry anti-robocall working groups
- Information sharing with trusted industry partners regarding emerging threats
- Support for development of new anti-robocall technologies and standards

8. INCIDENT RESPONSE AND REMEDIATION

8.1 Incident Detection and Response

Detection Methods:

- Automated monitoring system alerts
- Customer complaints and reports
- Industry partner notifications
- Regulatory agency notifications

Response Procedures:

1. Immediate investigation of reported incidents
2. Traffic analysis and pattern identification
3. Coordination with affected customers
4. Implementation of blocking or filtering measures
5. Documentation of actions taken
6. Follow-up monitoring to ensure effectiveness

8.2 Customer Notification and Remediation

When illegal robocalling is identified:

- Immediate notification to affected customer
- Suspension of traffic pending resolution
- Required customer remediation plan
- Monitoring of subsequent traffic patterns
- Termination of service for repeat violations

9. REPORTING AND COMPLIANCE

9.1 Regulatory Reporting

- Maintain accurate records of all robocall mitigation activities
- Provide regular reports to regulatory agencies as required
- Document all traceback responses and investigation cooperation
- Track and report effectiveness metrics of mitigation measures

9.2 Internal Reporting and Review

- Monthly review of robocall mitigation program effectiveness
- Quarterly assessment of emerging threats and technology updates
- Annual comprehensive program review and update
- Executive-level oversight of program performance and compliance

10. STAFF TRAINING AND AWARENESS

10.1 Employee Training Programs

- Regular training for technical staff on robocall identification and mitigation
- Customer service training on proper handling of robocall complaints
- Legal and compliance training on applicable regulations
- Security awareness training on fraud detection and response

10.2 Ongoing Education

- Stay current with evolving robocall techniques and countermeasures
 - Participate in industry conferences and training programs
 - Maintain certification and professional development for key personnel
 - Regular review and update of internal procedures and protocols
-

11. TECHNOLOGY UPGRADES AND CONTINUOUS IMPROVEMENT

11.1 Technology Enhancement

Orbitel is committed to:

- Regular evaluation of new anti-robocall technologies
- Investment in network infrastructure upgrades to support advanced authentication
- Integration of artificial intelligence and machine learning for pattern detection
- Participation in pilot programs for emerging robocall prevention technologies

11.2 Program Evolution

- Continuous monitoring of program effectiveness
 - Regular updates based on regulatory changes and industry best practices
 - Incorporation of lessons learned from incidents and investigations
 - Benchmarking against industry standards and peer performance
-

12. PRIVACY AND DATA PROTECTION

12.1 Customer Privacy Protection

All robocall mitigation activities are conducted in compliance with:

- Applicable privacy laws and regulations
- Customer privacy expectations and contractual obligations
- Industry standards for call detail record handling
- Data retention and destruction policies

12.2 Information Sharing

Customer information is shared only:

- As required by law or regulatory obligation
 - With explicit customer consent
 - In aggregated, non-personally identifiable form for industry cooperation
 - Under appropriate confidentiality agreements and protections
-

13. CONTACT INFORMATION

Robocall Mitigation Contact:

Adalto Cesar Rodrigues Silva, Technical Director
Orbitel Telecom
SIG Qd. 03 - Bloco B - Entrada 99 - Sala 101-
Brasília - DF - ZIP 70.610.430
Phone: +55 61 3031-4100
Email: telefonia@orbitel.com.br

Legal/Compliance Contact:

Adalto Cesar Rodrigues Silva, Technical Director
Orbitel Telecom
SIG Qd. 03 - Bloco B - Entrada 99 - Sala 101-
Brasília - DF - ZIP 70.610.430
Phone: +55 61 3031-4100
Email: telefonia@orbitel.com.br

14. CERTIFICATION

Orbitel Telecom certifies that:

1. This robocall mitigation program will be implemented across all applicable portions of our network;
 2. We are committed to full compliance with 47 CFR § 64.6305 and all applicable robocall mitigation requirements;
 3. We will cooperate fully with all traceback requests and investigations from the FCC, law enforcement, and industry partners;
 4. We will maintain and continuously improve this program based on emerging threats, technologies, and regulatory requirements;
 5. All information provided in this filing is true and accurate to the best of our knowledge.
-

Submitted by: Adalto Cesar Rodrigues Silva,
Technical Director, Orbitel Telecom
Brasilia, 05/28/2025

This document constitutes Orbitel Telecom's comprehensive robocall mitigation program as required by 47 CFR § 64.6305. It will be updated periodically to reflect changes in technology, regulations, and industry best practices.