

Robocall Mitigation Plan

1. Introduction

ISP CORP, as a foreign-based voice service provider, is committed to preventing abusive and malicious calls across our network. While we do not have a direct relationship with the Federal Communications Commission (FCC) in the United States, we recognize the global impact of unwanted calls, including robocalls, and the importance of implementing robust mitigation practices. This plan outlines the measures ISP CORP employs to ensure the integrity of our voice traffic and comply with all local laws and regulations in Peru, under the oversight of the competent telecommunications authorities in our country.

2. Contractual Requirements and Prohibitions

All customer agreements explicitly prohibit the origination of unlawful or abusive calls, including those that violate consumer protection laws or engage in fraudulent caller ID spoofing. Our service terms require customers to maintain traffic characteristics consistent with legitimate usage and to cooperate fully in any investigations regarding their traffic. We monitor key traffic metrics such as Answer-Seizure Ratio (ASR) and Average Call Duration (ACD). Deviations from expected thresholds may trigger enhanced review, service suspension, or termination.

3. Customer Onboarding and KYC Verification

ISP CORP employs a robust Know Your Customer (KYC) process before activating any outbound calling services. New customers must submit detailed business verification documentation and a comprehensive traffic profile, including the nature, purpose, estimated volumes, and end-user categories of their calls. This information is thoroughly reviewed by our internal compliance team to validate identity, confirm legitimate use cases, and assess potential risks. Outbound capabilities are enabled only after successful review and the customer formally acknowledges all compliance obligations, including the prohibition of illegal and abusive call activity.

4. Traffic Monitoring and Response to Malicious Activity

We maintain a continuous traffic monitoring program designed to detect and respond to unlawful or suspicious call behavior. Our systems identify indicators such as unusually short call durations, high call volumes over short periods, sequential or patterned dialing, and invalid Caller ID (CLI) formats. All outbound calls undergo CLI validation against E.164 formatting standards; anomalous CLIs are rejected and flagged for investigation.

Upon identifying suspicious activity, our compliance team immediately initiates an investigation. The customer is formally contacted and required to justify or remediate the flagged traffic. Failure to provide a satisfactory explanation or remediation may result in immediate suspension or termination of service. We fully cooperate with legitimate investigative efforts and may share relevant information, in accordance with applicable Peruvian laws and data protection obligations, to aid in the identification and mitigation of malicious call sources. All investigations and actions taken are logged for auditability.

5. Compliance with Local Regulations and Best Practices

ISP CORP operates in full compliance with all telecommunications laws and regulations in Peru. We are subject to oversight and fiscalization by the competent telecommunications authorities of the country. We implement internal best practices aligned with global efforts to combat unwanted calls. Our practices are designed to ensure call path accountability within our network and prevent the origination or transit of malicious traffic. We expect our partners and customers to comply with all applicable regulations in their respective jurisdictions, including those of the FCC for U.S.-bound traffic, as a prerequisite for service.

6. Customer Awareness and Policy Governance

Our framework includes structured internal training for relevant teams on detecting and managing suspicious traffic. This Robocall Mitigation Plan is reviewed at least annually, or sooner if required by new local regulations, emerging threats, or industry best practices. We share usage guidelines with customers to promote ongoing compliance and risk mitigation, fostering a shared understanding of legal and technical obligations to strengthen our voice traffic ecosystem.

7. Corporate Ownership and Affiliations

ISP CORP certifies that we are a standalone legal entity with no parent company or affiliated voice service entities. We have no previous business names or additional DBAs.

8. Conclusion

This Plan outlines ISP CORP's commitment to preventing unlawful and abusive call traffic. Our multi-faceted mitigation strategy includes rigorous KYC, clear contractual prohibitions, continuous traffic monitoring and CLI validation, and prompt response to malicious activity. We are dedicated to the ongoing execution, periodic review, and continuous improvement of this Plan, ensuring the integrity of our network and contributing to a safer telecommunications environment in line with Peruvian regulations and global best practices.