

ROBOCALL MITIGATION PROGRAM

Robocall Prevention, Caller Authentication, and Traffic Integrity Policy

Company Name: _____

DBA (if applicable): _____

Address: _____

Contact Email: _____

Contact Phone: _____

1. Purpose

This Program documents the policies, procedures, and safeguards implemented to prevent illegal robocalls, unlawful spoofing, or non-compliant telecommunications traffic in accordance with the TCPA, Truth in Caller ID Act, FCC rules, and 47 CFR §64.6305.

2. Service Description

TelecomPlus provides hosted PBX, SIP, and telecommunications services utilizing the SkySwitch hosted PBX platform. Services are intended solely for lawful business communications and not for robocalling or mass automated campaigns are to be used by TelecomPlus clients or affiliations.

3. Customer Verification & Written Compliance

Customers are verified for legitimacy prior to activation. Written agreements prohibit illegal robocalling, spoofing, traffic pumping, and TCPA violations. Violations result in immediate suspension or termination of service from TelecomPlus.

4. Caller ID & DID Integrity

All assigned DIDs are registered to verified customers. Only authorized numbers may be presented as Caller ID. Anonymous, spoofed, or misleading identification is prohibited.

5. Platform Compliance (SkySwitch)

The Company operates within the SkySwitch hosted PBX environment and adheres to all applicable acceptable use policies and anti-abuse safeguards. Where SkySwitch maintains compliance consistent with 47 CFR §64.6305(c), the Company maintains equivalent compliance.

6. Traffic Monitoring & Mitigation

Ongoing monitoring identifies abnormal call behavior. Suspicious traffic is investigated, blocked, or suspended. The Company cooperates with traceback requests and regulatory authorities.

7. STIR/SHAKEN Call Authentication & Attestation

The Company implements STIR/SHAKEN caller authentication wherever technically feasible. Calls are signed and verified to ensure integrity and reduce spoofing risks. Attestation levels are applied as follows: A Attestation – Full relationship with customer and validated right to use the calling number; B Attestation – Known customer but number ownership not fully verified; C Attestation – Gateway or transit traffic. Digital certificates are maintained through approved certificate authorities. Where the platform supports it, calls are cryptographically signed to ensure downstream verification.

8. Complaint Handling & Traceback Cooperation

A designated abuse contact handles complaints promptly. The Company cooperates with carriers, industry traceback groups, and law enforcement.

9. Enforcement

Confirmed violations may result in call blocking, suspension, termination, and reporting to authorities. The Company maintains a zero-tolerance policy for illegal robocalls.

10. Review & Updates

This Program is reviewed periodically and updated to reflect regulatory or technical changes.

11. Certification

The undersigned certifies that this Robocall Mitigation Program is implemented and maintained in good faith to comply with FCC regulations and 47 CFR §64.6305.

Authorized Representative Name: _____

Title: _____

Signature: _____

Date: _____