



Robocall Mitigation Program Description

Robocall Mitigation Plan

Company Name: Network Innovation Solutions

Platform: Hosted 3CX PBX in Microsoft Azure / 3CX Hosting

Upstream Voice Carriers: Bandwidth.com and Sangoma

STIR/SHAKEN Signing Provider: Telonium Wholesale

Effective Date: February 12, 2026

Program Overview:

Network Innovation Solutions, Corp. is committed to following FCC regulations under 47 C.F.R. § 64.6305 and the TRACED Act.

Corrective Filing – FCC Robocall Mitigation Database

Action or Investigation Description:

Network Innovation Solutions, Corp. (OCN 948L) was the subject of a formal Enforcement Bureau Removal Order issued on August 25, 2025, in DA 25-737. In that Order, NIS was listed in Appendix A and was removed from the Robocall Mitigation Database (RMD) because it did not update its RMD certification and robocall mitigation plan by the required February 26, 2024 deadline, as mandated under 47 C.F.R. § 64.6305.

Following removal, NIS conducted an internal compliance review and submitted a corrective filing that included a fully updated robocall mitigation plan and updated certification information. On August 29, 2025, the Enforcement Bureau provisionally reinstated NIS's filing in the RMD, subject to the requirement that additional revisions be completed to bring the filing into full compliance with Commission rules.

NIS has completed the required updates, including enhanced Know Your Customer (KYC) procedures, expanded mitigation language, third-party analytics details, traceback participation commitments, and updated compliance disclosures consistent with Subpart HH of 47 C.F.R.

On January 7, 2026, NIS was informed that the Enforcement Bureau had reviewed our updates to the Robocall Mitigation Database and converted NIS's status from "provisional reinstatement" to "full reinstatement."

Summary

STIR/SHAKEN Status:

NIS is a non-facilities-based interconnected VoIP provider providing hosted VoIP phone systems using 3CX PBX servers deployed in Microsoft Azure or hosted directly by 3CX. NIS is registered with the Secure Telephone Identity Policy Administrator (STI-PA) and holds a valid SHAKEN certificate issued by an approved STI Certification Authority.

NIS performs STIR/SHAKEN authentication and attestation for all IP-based outbound voice traffic. Call signing is performed through Telonium Wholesale signing services prior to routing traffic to our upstream carriers, Bandwidth.com and Sangoma. Carrier-side STIR/SHAKEN signing has been disabled to ensure a single authoritative Identity header is applied. NIS maintains direct control over attestation decisions.

NIS does not originate high-volume or mass autodialed traffic and prohibits such activity absent documented lawful use and customer consent. We maintain an Acceptable Use Policy and review any complaints of robocalling activity. Any user found violating our policy will have their service suspended or terminated immediately.

Robocall Mitigation Practices

- **Know Your Customer (KYC):** Verify the identity and legitimacy of all new and existing customers. NIS implements a detailed KYC program applied to both new and existing customers. Verification includes:
 - Legal business verification
 - EIN validation
 - Government ID verification
 - Website and operations review
 - Business purpose and use-case vetting
 - Annual revalidation
 - Mandatory re-screening when traffic anomalies occur
- **Traffic Monitoring & Analytics:** NIS continuously monitors VoIP traffic through the PBX and upstream providers. NIS relies on upstream carrier analytics and fraud detection and supplements this with 3CX analytics. NIS uses:
 - 3CX call analytics
 - Upstream carrier fraud analytics (Bandwidth and Sangoma)
 - IP authentication
 - PBX firewall protections
 - Call spike and pattern detection
 - International calling disabled by default
- **Reasonable Steps to Mitigate Illegal Traffic:** NIS performs:
 - Immediate log review upon detection
 - Destination blocking
 - Traffic throttling
 - Mandatory KYC refresh
 - Full suspension for confirmed violations
 - NIS responds fully and within 24 hours to all traceback requests from the Commission, law enforcement, or the Industry Traceback Group.
- **Prohibited Uses:** Customers may not:
 - Originate illegal robocalls
 - Use autodialers without consent documentation



o Spoof caller ID

o Generate short-duration repetitive traffic patterns

o Use APIs for automated calling without authorization

- Call Blocking: Users cannot perform robocalling without a third-party API integration into the Hosted PBX which would require technical assistance. No end-user is authorized with this level of access to the Hosted PBX.
- Additional Mitigations:
 - o NIS only routes outbound traffic through upstream providers registered in the FCC Robocall Mitigation Database. (Bandwidth and Sangoma).
 - o NIS has implemented a concurrent call limit on its Hosted PBXs.
 - o NIS's PBX has blacklisting enabled at the global level and at the PBX level.
 - o NIS has enabled global spam protection updated daily.
 - o International calling is disabled by default. Clients must provide a business usage case for international calling within specific regions.
 - o NIS disables direct SIP and IP calling.
 - o NIS authenticates SIP signaling from its PBXs, the Telonium signing proxy, and upstream carriers (Bandwidth.com and Sangoma). No other SIP communication is authorized.
 - o Anti-hacking enabled PBX firewalls to lock out invalid login attempts.
- Governance & Compliance
 - o NIS will update its Robocall Mitigation Database filing within 10 business days of any material operational, signing, carrier, or mitigation change consistent with 47 C.F.R. § 64.6305.
 - o NIS maintains internal documentation of SHAKEN certificate validity, SPC token management, and signing architecture and conducts periodic compliance reviews.

STIR/SHAKEN Governance Statement:

NIS is not claiming exemption under 47 C.F.R. § 64.6305(d)(2)(i). NIS actively implements STIR/SHAKEN authentication and attestation in accordance with FCC rules. Certificate management, SPC token access, and signing architecture are tracked and maintained internally. NIS updates its Robocall Mitigation Database (RMD) filing within 10 business days of any material change.

Point of Contact:

Name: James Thomas

Title: Chief Operating Officer

Email: jthomas@gonis.us



Network Innovation Solutions Hosted PBX VOIP Telephone Service Acceptable Usage Policy

1. Purpose

This policy outlines the acceptable use of telephone services provided by Network Innovation Solutions to ensure responsible use, control costs, maintain productivity, and comply with legal obligations.

2. Scope

This policy applies to all employees, customers, clients, companies, contractors, and authorized users of Network Innovation Solutions' telephone services, including landlines, mobile phones, and voicemail systems.

3. Acceptable Use

- Telephone services are provided for conducting company business.
- Limited personal use is permitted on an occasional basis if it does not interfere with work duties or result in excessive costs.
- Users must respect confidentiality and privacy during telephone communications.

4. Prohibited Use — General

Users shall not:

- Use telephone services for unlawful or fraudulent activities.
- Make excessive personal calls or use the services for non-business solicitation.
- Engage in harassment, offensive, discriminatory, or obscene communications via telephone or voicemail.
- Record or monitor calls without proper authorization.
- Use services to transmit confidential or proprietary information without security safeguards.
- Bypass telephone service controls or access unauthorized features.
- Use telephone services in violation of any other company policies or applicable laws.

5. Prohibited Uses — Robocalling

Users are strictly prohibited from:

- Using the telephone service for any illegal robocalling activities including violations of federal and state telecommunication laws.
- Making calls using pre-recorded messages or non-live human interactions without proper consent.
- Participating in or operating continuous, persistent, or excessive calls or message campaigns that harass or annoy recipients.
- Using the service for spoofing caller ID, or sending calls through unallocated or invalid telephone numbers.
- Failing to monitor calling campaigns to minimize complaints and prevent excessive or repetitive calling to the same number or destination within a short period.

- Recording or monitoring phone calls without securing required consent per applicable laws.
- Operating call centers, chat lines, or conference lines without explicit authorization.
- Transmitting or receiving broadcasts, recorded materials, or extensive call forwarding intended to facilitate robocalling or spam calls.

6. Monitoring and Privacy

- Telephone calls and voicemail messages may be monitored, recorded, and audited by Network Innovation Solutions for quality assurance, compliance, and security purposes.
- Monitoring will be performed in accordance with applicable privacy laws and company guidelines.
- Monitoring and recording will comply with applicable federal and state consent laws.

7. User Responsibilities

- Safeguard access to telephones and voicemail systems.
- Report lost or stolen devices immediately to [Contact/IT Support].
- Use telephone services responsibly, avoiding excessive or inappropriate use.
- Adhere to this policy and report any violations.

8. Consequences of Non-Compliance

Violations of this policy may result in:

- Disconnection or restriction of telephone service.
- Disciplinary action, up to and including termination of employment.
- Legal action if warranted.

9. Review and Updates

This policy will be reviewed annually and updated as necessary to reflect changes in laws, technology, and business needs.