



PBX Robocall Safeguards and Procedures

Hospitality WiFi International manages its PBX using several SIP providers, including IDT/net2phone. We actively communicate and collaborate with our partners to ensure compliance with STIR/SHAKEN. As part of our commitment to preventing illegal robocalls, we have implemented a number of procedures to safeguard our PBX and respond to any security concerns.

Steps taken to prevent Illegal Robocalls:

PBX Access Controls:

- Limited Administrative Access: Only select system administrators have the ability to create and modify extensions and trunk entries within the PBX. All other users have read-only access, limited to monitoring and reporting.
- Network Connectivity Restrictions: Access to the PBX administration interface is restricted via access control lists and can only be accessed through a VPN connection.
- Credential Management:
 - o Extension-Level Passwords: Passwords for PBX extensions are autogenerated and complex. These passwords are reset as required during extension deployment or upon administrative need.
 - o Device-Level Admin Credentials: Admin credentials for devices (such as desk sets) are also autogenerated and complex. These passwords are reset whenever devices are redeployed or reassigned.
- Softphone Security: Virtual softphones are secured using best-practice workstation and network-level security measures. Upon deactivation of a softphone user, the associated PBX extension password is reset with a complex, auto-generated password.

Proactive Call Monitoring:

- Active Dashboard Monitoring: Several users monitor a live dashboard that displays incoming and outgoing calls.
- Incident Response: If suspicious traffic is detected, the specific instances are immediately reviewed. Access may be revoked until a deeper investigation is completed.
- Collaboration with SIP Providers: Any reports from call recipients or SIP providers regarding potential suspect traffic from our PBX or leased numbers are promptly investigated by system administrators. Remedial actions are taken as needed, which may include restricting access to the PBX for any offending device or extension.

Automated ("Robocall") Call Services:

- Hospitality WIFI International does **NOT** currently have any automated or "robocall" services in place, and there are **NO PLANS** to implement such services in the future.

We confirm that all reports related to suspect traffic will be investigated thoroughly and acted upon as necessary to ensure continued compliance and security.

Additional Technical Safeguards

- Anonymous SIP traffic is disabled.
- Outbound routing policies restrict international dialing to approved destinations.
- Monitoring alerts are generated for outbound calls to unapproved international destinations.
- Automated intrusion detection and blocking mechanisms are deployed to prevent unauthorized SIP registration attempts and brute-force attacks.
- A designated robocall mitigation contact is actively monitored, and the company commits to respond fully within 24 hours to traceback requests from the Federal Communications Commission, law enforcement agencies, and the industry traceback consortium.