

Espericon Acceptable Use Policy (AUP) – Robocall Mitigation and FCC Compliance

1. Purpose

This Acceptable Use Policy ("Policy") sets forth the acceptable use of telecommunications services provided by **Espericon** ("Provider") to ensure compliance with the Federal Communications Commission (FCC) regulations, particularly those aimed at mitigating unlawful robocalls. This Policy forms an integral part of Espericon's **Robocall Mitigation Plan (RMP)** and applies to all customers, users, and affiliated third parties.

2. Scope

This Policy applies to:

- All voice service customers, including residential, business, and wholesale clients
- Resellers, agents, and downstream carriers using Espericon's services
- Vendors, contractors, and technology partners connected to our voice network
- Any party accessing or utilizing Espericon's voice or messaging platforms

3. Prohibited Activities

Users of Espericon services must refrain from engaging in the following prohibited activities:

3.1 Illegal Robocalls

- Initiating or facilitating unlawful robocalls or autodialed calls that violate the **Telephone Consumer Protection Act (TCPA)** or FCC regulations.
- Distributing prerecorded messages or initiating bulk call campaigns without proper consent from the recipients.

3.2 Caller ID Manipulation

- Using false, misleading, or spoofed caller ID information with the intent to defraud, harm, or wrongfully obtain anything of value.
- Failing to transmit accurate caller identification as required by law.

3.3 Suspicious Calling Patterns

- Generating high-volume or short-duration calls in patterns typical of illegal robocalling operations.
- Using Espericon's services to deliver traffic from known robocall sources or campaigns.

4. Robocall Mitigation Responsibilities

All customers and downstream providers are expected to:

- Provide accurate and complete caller identity information.
- Cooperate with Espericon's implementation of **STIR/SHAKEN** call authentication frameworks.
- Respond to traceback requests from the **Industry Traceback Group (ITG)**, FCC, or law enforcement in a timely manner.
- Submit and maintain a robocall mitigation plan if required under FCC rules (47 CFR § 64.6305).

5. Monitoring and Enforcement

Espericon reserves the right to:

- Monitor network usage and call patterns to detect violations of this Policy.
- Block, reroute, or terminate traffic that is in violation of FCC rules or this Policy.
- Suspend or terminate accounts involved in prohibited behavior.
- Report non-compliant activity to the FCC, ITG, and other appropriate authorities.

6. Reporting Violations

Violations or suspected misuse of Espericon's network can be reported to our Compliance Team at **compliance@espericon.com** or through our abuse reporting page: [<https://www.espericon.com/abuse-reporting>].

7. Policy Updates

Espericon may update this Policy periodically to reflect changes in law, regulation, or industry best practices. The latest version will always be available at: [<https://www.espericon.com/aup>]

8. Acknowledgment

By using Espericon's services, you agree to comply with this Acceptable Use Policy. Violations may result in service suspension, termination, and legal action.