

Acceptable Use Policy

Effective Date: October 6, 2026

This Acceptable Use Policy ("AUP") governs the use of telecommunications, voice, messaging, telephone number, SIP trunking, hosted communications, application programming interface ("API"), software, cloud communication and related services (collectively, the "Services") provided by Instacall LLC, including its affiliates, suppliers and underlying service providers ("Instacall," "we," "us," or "our").

This AUP forms part of the agreement between Instacall and each customer, reseller, user, subscriber or other person or entity that accesses or uses the Services ("Customer" or "you").

By using the Services, Customer agrees to comply with this AUP and all applicable federal, state, local and international laws, regulations, regulatory requirements and industry rules.

01 General Compliance Requirement

Customer may use the Services only for lawful purposes.

Customer is solely responsible for ensuring that all communications initiated, transmitted, received or facilitated through the Services comply with applicable law.

Without limitation, Customer must comply, where applicable, with:

- the Telephone Consumer Protection Act ("TCPA"), 47 U.S.C. § 227;
- Federal Communications Commission ("FCC") rules and orders;
- the Telemarketing Sales Rule ("TSR"), 16 C.F.R. Part 310;
- Federal Trade Commission ("FTC") requirements;
- the Truth in Caller ID Act and related FCC regulations;
- federal and state Do Not Call requirements;
- applicable state telemarketing, telephone solicitation, privacy, call-recording and consumer-protection laws;
- applicable SMS, MMS and commercial messaging requirements;
- applicable carrier, aggregator and messaging ecosystem requirements;
- STIR/SHAKEN and robocall-mitigation requirements applicable to the traffic being originated or transmitted;
- and
- any other law, regulation, order or industry requirement applicable to Customer's communications.

Customer is responsible for determining which requirements apply to its business, communications, campaigns, recipients and jurisdictions.

Instacall does not provide legal advice, and provision of the Services does not constitute confirmation that Customer's intended use is lawful.

02 Prohibited Use

Customer may not use, or permit any person to use, the Services for unlawful, fraudulent, deceptive, abusive or harmful activity.

Prohibited activity includes, without limitation:

- fraud, scams, impersonation or deceptive business practices;
- transmitting communications intended to defraud or mislead recipients;
- phishing, credential theft or identity theft;
- harassment, threats, intimidation or abusive communications;
- communications intended to cause harm or unlawfully obtain money, property, information or anything of value;
- unlawful robocalls or robotexts;
- unlawful prerecorded, artificial-voice or AI-generated voice calls;
- communications made without legally required consent;
- communications to recipients where applicable law prohibits such communications;
- communications that disregard a valid revocation of consent, opt-out request or Do Not Call request;
- illegal or deceptive advertising or promotions;
- transmitting malware, malicious links or harmful software;
- facilitating criminal activity;
- impersonating a government agency, financial institution, healthcare provider, law-enforcement organization or another person or business without authorization;
- interfering with telecommunications networks or other users;
- intentionally generating nuisance, abusive or artificially inflated traffic; or
- attempting to circumvent Instacall's fraud, compliance, security or traffic-management controls.

Customer may not use the Services to assist another person in engaging in prohibited activity.

03 Voice Communications

All voice traffic transmitted through Instacall must have a legitimate and lawful purpose.

Customer is responsible for ensuring that outbound and inbound voice communications satisfy all applicable FCC, FTC, TCPA, TSR, Do Not Call, consumer-protection and state-law requirements.

Instacall prohibits voice traffic that constitutes or facilitates:

- illegal robocalling;
- fraudulent or deceptive calling;

- unauthorized prerecorded or artificial-voice calling;
- unlawful use of automatic dialing technology;
- harassment or repeated abusive calling;
- unauthorized solicitation;
- caller-ID manipulation intended to deceive, defraud or cause harm;
- traffic designed to evade carrier, analytics, regulatory or enforcement systems; or
- other unlawful calling activity.

Nothing in Instacall's provisioning of telephone numbers, SIP trunks, dialing capacity, routing, caller-ID capability or other telecommunications resources constitutes authorization for Customer to initiate any particular communication.

04 TCPA Compliance

Customer is solely responsible for compliance with the TCPA and FCC rules implementing the TCPA.

Where consent is required by applicable law, Customer must possess legally sufficient consent before initiating the applicable communication.

Customer must be able to demonstrate the existence and validity of required consent upon reasonable request from Instacall, a telecommunications carrier, industry partner, regulator or other authorized entity.

Customer must honour legally valid:

- consent revocations;
- opt-out requests;
- company-specific Do Not Call requests; and
- other requests to cease communications.

Customer may not use Instacall Services to circumvent TCPA restrictions through alternate telephone numbers, multiple accounts, third-party identities, number rotation, caller-ID manipulation or other methods.

05 Artificial, Prerecorded and AI-Generated Voice

For purposes of this AUP, artificial or prerecorded voice communications include communications utilizing technology that generates or reproduces a human voice, including AI-generated or synthetically generated voices where applicable under FCC rules.

Customer may not use artificial, prerecorded, synthetic, cloned or AI-generated voice technology through the Services where such use violates the TCPA, FCC rules or other applicable law.

Customer is solely responsible for obtaining any consent required for such communications.

Voice cloning or artificial voice technology may not be used to:

- impersonate another individual without authorization;

- misrepresent the identity of the caller;
- deceive a recipient;
- commit fraud;
- wrongfully obtain anything of value; or
- otherwise violate applicable law.

06 Do Not Call Compliance

Customer is responsible for compliance with all applicable federal and state Do Not Call requirements.

Customer must not use the Services to contact persons where the communication is prohibited by:

- the National Do Not Call Registry;
- applicable state Do Not Call registries;
- company-specific Do Not Call requests; or
- any other legally applicable suppression requirement,

except where Customer has a valid legal basis permitting the communication.

Instacall may require Customer to provide evidence of its compliance procedures, consent records, suppression practices or other relevant documentation.

07 FTC and Consumer-Protection Compliance

Customer may not use Instacall Services for conduct prohibited by the FTC Act, the Telemarketing Sales Rule or other applicable consumer-protection laws.

Customer may not engage in:

- deceptive or misleading representations;
- fraudulent sales practices;
- unauthorized billing;
- material misrepresentations concerning products or services;
- misleading claims regarding identity or affiliation;
- abusive communications;
- unlawful payment practices;
- schemes designed to obtain money or information through deception; or
- other unfair or deceptive acts or practices.

Customer remains responsible for determining whether the FTC's Telemarketing Sales Rule or another regulatory framework applies to its activities.

08 Caller ID and Number Usage

Customer must have the legal right or authorization to use any telephone number presented as caller identification.

Customer may not knowingly transmit misleading or inaccurate caller-ID information with the intent to defraud, cause harm or wrongfully obtain anything of value.

Prohibited practices include:

- unauthorized use of another person's telephone number;
- impersonating unrelated businesses through caller ID;
- using invalid or fabricated caller-ID information;
- manipulating caller ID to facilitate fraud or deception;
- unauthorized number substitution;
- number rotation designed to circumvent blocking, reputation systems or regulatory enforcement; and
- intentionally interfering with caller-ID authentication mechanisms.

Where Customer places calls on behalf of another entity, Customer must possess appropriate authorization to represent that entity and to use any telephone number associated with it.

09 STIR/SHAKEN and Call Authentication

Customer must not take any action intended to falsify, defeat, circumvent or improperly influence STIR/SHAKEN authentication or other call-authentication mechanisms.

Customer must provide accurate information requested by Instacall regarding:

- Customer's identity;
- ownership or authorization to use telephone numbers;
- the source and destination of traffic;
- end users or downstream customers;
- traffic purpose;
- calling applications;
- originating networks; and
- other information reasonably necessary for regulatory or robocall-mitigation compliance.

Instacall may determine the appropriate call-attestation treatment or other authentication handling based on applicable standards, information available to Instacall and Customer's authorization to use the calling number.

Customer may not demand or attempt to obtain an authentication level for which its traffic does not qualify.

10 SMS and MMS Messaging

All SMS and MMS traffic transmitted using Instacall Services must comply with applicable federal and state law, FCC requirements, TCPA requirements and applicable carrier and messaging ecosystem rules.

Customer is responsible for:

- having an appropriate legal basis for each message;
- obtaining and maintaining required consent;
- maintaining sufficient evidence of required consent;
- accurately identifying the business, organization or other party responsible for the communication where required;
- honouring legally valid opt-out and consent-revocation requests;
- preventing further communications when continued messaging is prohibited;
- complying with applicable messaging registration and campaign-verification requirements; and
- ensuring that the content and purpose of messaging traffic corresponds with any registered or approved messaging use case.

Customer may not send unsolicited or unlawful bulk messaging through the Services.

11 Messaging Registration and Campaign Integrity

Where telecommunications carriers, messaging aggregators or industry programs require registration, verification or approval of messaging traffic, Customer must provide complete and accurate information.

Customer may not:

- provide false campaign information;
- register one use case while transmitting materially different traffic;
- use another entity's identity without authorization;
- share approved messaging campaigns with unauthorized third parties;
- evade messaging registration requirements;
- rotate numbers to bypass filtering or blocking;
- modify traffic for the purpose of avoiding carrier enforcement; or
- continue transmitting traffic that has been suspended or prohibited by a carrier or regulator.

Instacall may suspend messaging traffic that is unregistered, improperly registered or inconsistent with the represented use case.

12 SMS Prohibited Content and Conduct

Customer may not use messaging Services for:

- scams or fraud;
- phishing;
- deceptive financial solicitations;
- impersonation;
- illegal goods or services;
- unlawful debt collection;
- malicious links or malware;
- unlawful controlled-substance promotion;
- unlawful gambling activity;
- threats, harassment or hate-based abuse;
- content that violates applicable law;
- snowshoe messaging or similar techniques designed to circumvent filtering;
- unlawful lead-generation messaging;
- purchased, rented, harvested or otherwise unlawfully obtained recipient lists where required consent is absent; or
- messaging intended to defeat spam-prevention or carrier-compliance systems.

Carriers and messaging partners may maintain additional prohibited-content categories. Customer agrees to comply with those requirements when using networks subject to such restrictions.

13 Consent and Compliance Records

Customer is responsible for maintaining records reasonably sufficient to demonstrate the legality of its communications.

Depending on the nature of the traffic and applicable laws, such records may include:

- consent records;
- consent language;
- date and method of consent;
- source of recipient information;
- campaign information;
- opt-out and revocation records;
- Do Not Call suppression information;
- customer or end-user identification;
- telephone number ownership or authorization;

- messaging registration information; and
- other records required by applicable law.

Instacall may request relevant documentation when investigating complaints, traceback requests, suspected unlawful activity or regulatory inquiries.

Failure to provide reasonably requested compliance information may result in restriction or suspension of Services.

14 Lead Generation and Third-Party Data

Customer is solely responsible for the lawful collection, purchase, acquisition and use of telephone numbers, leads, consumer data and contact information.

The fact that a third party represents that data is "opted in," "TCPA compliant," "DNC scrubbed," "consented," or otherwise compliant does not relieve Customer of its own legal obligations.

Customer may not knowingly use data obtained through:

- unlawful harvesting;
- fraud;
- deceptive consent mechanisms;
- unauthorized data access; or
- any other unlawful method.

Customer is responsible for confirming that any consent upon which it relies legally permits the specific communications it conducts.

15 Call Recording and Monitoring

Customer is responsible for complying with all federal and state laws applicable to recording, monitoring, transcribing or analyzing telephone calls and other communications.

Where notice or consent is legally required before recording or monitoring a communication, Customer is solely responsible for obtaining it.

The availability of recording or transcription functionality within an Instacall product does not represent a determination that its use is lawful in any particular jurisdiction.

16 Privacy and Personal Information

Customer must process personal information using the Services in accordance with applicable privacy and data-protection laws.

Customer may not use the Services to unlawfully collect, disclose, sell, transmit, access or otherwise process personal information.

Customer is responsible for providing legally required privacy notices and obtaining legally required permissions for Customer's collection and processing of personal information.

17 Fraud and Impersonation

Instacall maintains a zero-tolerance policy toward telecommunications fraud.

The Services may not be used in connection with:

- government impersonation scams;
- financial institution impersonation;
- technical-support scams;
- healthcare scams;
- insurance scams;
- identity theft;
- account-takeover schemes;
- credential harvesting;
- fraudulent lead-generation schemes;
- fraudulent payment requests;
- voice-cloning scams;
- deceptive caller-ID practices;
- phishing or smishing; or
- any comparable fraudulent activity.

Instacall may immediately suspend traffic reasonably suspected of being connected with fraud.

18 Traffic Manipulation and Network Abuse

Customer may not engage in activity designed to artificially generate, inflate, manipulate or misrepresent telecommunications traffic.

Prohibited conduct includes:

- artificial traffic inflation;
- traffic pumping;
- unauthorized revenue-share traffic;
- Wangiri or one-ring fraud;
- intentional short-duration traffic intended to manipulate billing;
- fraudulent answer supervision;
- call looping;
- traffic intended primarily to generate carrier compensation;

- denial-of-service activity;
- excessive signaling intended to impair network operations; and
- attempts to bypass routing, fraud or security controls.

19 Resellers and Downstream Customers

Customers that resell, sublicense, provide access to or otherwise permit third parties to use Instacall Services are responsible for their downstream users.

Resellers must take reasonable measures to know and verify their customers and to prevent unlawful use of the Services.

Customer remains responsible to Instacall for traffic originated by its customers, end users, agents, contractors and downstream providers.

Instacall may request information identifying the person or entity responsible for particular traffic.

Customer may not intentionally conceal the true originator, beneficial user or purpose of traffic.

20 Know Your Customer and Verification

Instacall may require identity, business and compliance information before or during the provision of Services.

Requested information may include:

- legal business name;
- incorporation or registration information;
- business address;
- ownership information;
- government-issued identification;
- website information;
- intended use of Services;
- sample communications or campaign information;
- customer or downstream-user information;
- consent information;
- proof of telephone-number authorization; and
- other information reasonably necessary for compliance or fraud prevention.

Customer must provide accurate, complete and current information.

Instacall may decline, restrict or discontinue Services if required verification cannot be completed satisfactorily.

21 Regulatory and Industry Cooperation

Instacall may cooperate with lawful requests from:

- the FCC;
- the FTC;
- law-enforcement agencies;
- state attorneys general;
- courts;
- regulatory agencies;
- the Industry Traceback Group;
- originating, intermediate and terminating carriers;
- messaging aggregators;
- telephone-number providers; and
- other authorized parties investigating suspected unlawful communications.

Customer agrees to reasonably cooperate with investigations concerning traffic transmitted through its account.

Where permitted or required by law, Instacall may provide information concerning Customer, its account, its traffic or its downstream users in response to valid legal, regulatory, traceback, fraud-prevention or network-security requests.

22 Traceback Requests

Customer must cooperate promptly with legitimate traceback investigations involving traffic carried through Instacall.

Instacall may require Customer to identify:

- the source of traffic;
- the originating customer or end user;
- the purpose of the traffic;
- the calling party;
- associated telephone numbers;
- upstream or downstream providers; and
- other relevant traffic information.

Failure to cooperate with a traceback investigation may result in immediate suspension or termination.

23 Complaints and Traffic Reputation

Instacall may investigate traffic associated with:

- consumer complaints;
- FCC or FTC complaints;
- carrier complaints;
- spam or scam classifications;
- elevated blocking;
- excessive opt-outs;
- fraud indicators;
- traceback requests;
- invalid caller identification;
- messaging violations;
- abnormal traffic patterns; or
- other indicators of potentially unlawful or abusive activity.

Instacall is not required to conclusively establish a legal violation before taking reasonable action to protect its network, suppliers, customers or the public.

24 Monitoring

To the extent permitted by applicable law, Instacall may monitor network and traffic information for purposes including:

- network management;
- security;
- fraud prevention;
- abuse prevention;
- regulatory compliance;
- traceback cooperation;
- billing;
- quality assurance; and
- enforcement of this AUP.

Nothing in this section creates an obligation for Instacall to monitor every communication or independently verify Customer's compliance.

Customer remains solely responsible for its use of the Services.

25 Suspension, Blocking and Termination

Instacall may block traffic, restrict functionality, suspend Services or terminate an account when Instacall reasonably believes that:

- Customer has violated this AUP;
- traffic may violate applicable law;
- Customer presents an unacceptable fraud or compliance risk;
- continued traffic may harm Instacall's network or reputation;
- a carrier, supplier or regulator requests or requires action;
- Customer fails to respond to a compliance inquiry;
- Customer provides materially inaccurate information;
- Customer fails to cooperate with a traceback;
- traffic creates significant consumer complaints;
- telephone numbers or messaging campaigns are being misused; or
- immediate action is reasonably necessary to prevent harm.

Where circumstances reasonably permit, Instacall may provide Customer an opportunity to respond or remediate. Instacall may take immediate action without prior notice where necessary to address fraud, illegal traffic, regulatory requirements, network security or material risk.

26 Customer Responsibility

Customer is solely responsible for:

- its communications;
- communications initiated by its employees, contractors, agents and users;
- the legality of its contact lists and leads;
- required consent;
- regulatory registrations;
- suppression lists;
- the content of communications;
- representations made during communications;
- compliance by downstream customers; and
- maintaining evidence sufficient to establish compliance.

Instacall's acceptance, routing or completion of communications does not mean that Instacall has reviewed, approved or determined the communication to be lawful.

27 Changes in Law or Industry Requirements

Telecommunications laws, FCC and FTC rules, carrier requirements and industry standards change periodically.

Customer is responsible for maintaining ongoing compliance with requirements applicable to its use of the Services.

Instacall may modify this AUP when necessary to address changes in law, regulation, network requirements, carrier policies, security risks or business practices.

Continued use of the Services after an updated AUP becomes effective constitutes acceptance of the revised AUP to the extent permitted by applicable law.

28 No Waiver

Instacall's failure to enforce a provision of this AUP in one instance does not waive its right to enforce that provision or another provision in the future.

29 Relationship to Other Agreements

This AUP supplements Instacall's Terms of Use, service agreements, order forms and other applicable agreements.

If a provision of this AUP conflicts with a more specific written agreement between Customer and Instacall, the applicable agreement will control to the extent of the conflict, except where enforcement of this AUP is necessary to comply with law, regulation, carrier requirements, fraud-prevention obligations or network-security requirements.

30 Reporting Abuse

Suspected abuse of Instacall Services should be reported through Instacall's designated abuse-reporting channel available on the Instacall website.

Reports should include sufficient information to identify the relevant telephone number, message, call, date, time and nature of the suspected violation where available.

Instacall may investigate credible reports and take action consistent with this AUP.

31 Contact Information

Questions regarding this Acceptable Use Policy or compliance requirements applicable to use of Instacall Services may be submitted through Instacall's official contact channels.

Instacall LLC
930 Washington Avenue, Suite 210-22
Miami Beach, Florida 33139
United States

Telephone: (302) 271-9101

Email: compliance@instacall.digital

Website: instacall.digital

InstaCall