



Phone : 714-705-4929

Fax : 714-705-4930

Info@brightpacket.com

Your Partner for Business Telecommunications 11756 Artesia Blvd., Suite A, Artesia, CA 90701

Bright Packet, Inc.

Acceptable Use Policy (AUP)

Effective Date: July 16, 2026

1. Purpose

This Acceptable Use Policy ("AUP") describes the acceptable use of telecommunications and related services ("Services") provided by Bright Packet, Inc. ("Bright Packet"). This policy is intended to protect the integrity, reliability, and security of our network while ensuring compliance with applicable federal, state, and local laws and regulations.

This AUP forms part of Bright Packet's Terms and Conditions. Customers are responsible for ensuring that all authorized users comply with this AUP.

2. Compliance with Laws

Customers must use the Services only for lawful purposes and in compliance with all applicable laws and regulations, including but not limited to:

- Federal Communications Commission (FCC) regulations
- Telephone Consumer Protection Act (TCPA)
- Truth in Caller ID Act
- STIR/SHAKEN requirements
- FCC Robocall Mitigation requirements
- Any applicable state telecommunications regulations

Customers are solely responsible for ensuring that their use of the Services complies with all applicable legal requirements.

3. Prohibited Activities

The following activities are strictly prohibited:

Illegal Activities

- Any unlawful use of the Services
- Fraudulent or deceptive communications
- Criminal activity

- Unauthorized interception or monitoring of communications

Robocalling and Spam

Customers shall not use the Services to:

- Transmit illegal robocalls
- Send unsolicited telemarketing calls in violation of applicable law
- Generate excessive nuisance or spam calls
- Conduct voice phishing (vishing)
- Engage in scam or fraudulent calling campaigns

Caller ID Spoofing

Customers may not:

- Transmit misleading or fraudulent Caller ID information
- Falsify calling party information
- Misrepresent the origin of any communication

Legitimate Caller ID presentation consistent with applicable law is permitted.

Network Abuse

Customers shall not:

- Attempt unauthorized access to Bright Packet's network
- Interfere with network operations
- Launch denial-of-service attacks
- Distribute malware or malicious code
- Circumvent security controls

4. STIR/SHAKEN and Call Authentication

Customers must cooperate with Bright Packet in maintaining compliance with STIR/SHAKEN requirements and any applicable industry call authentication standards.

Bright Packet reserves the right to request additional information regarding calling practices when necessary to support compliance efforts.

5. Robocall Mitigation

Customers are responsible for ensuring that outbound traffic complies with applicable robocall mitigation requirements.

Bright Packet may monitor traffic patterns and investigate suspicious or potentially unlawful calling activity.

Customers must promptly respond to reasonable requests for information regarding their traffic or calling practices.

6. Customer Responsibilities

Customers agree to:

- Maintain accurate account information
- Protect account credentials
- Prevent unauthorized use of their Services
- Report suspected fraud or security incidents promptly
- Cooperate with investigations relating to abuse or illegal activity

7. Monitoring and Enforcement

Bright Packet may monitor network usage to protect the security and integrity of its network and to comply with legal and regulatory obligations to the extent permitted by applicable law.

If Bright Packet reasonably believes that a customer is violating this AUP, Bright Packet may take reasonable actions, including but not limited to:

- Issue a warning
- Suspend affected Services
- Block or restrict specific traffic
- Require corrective action
- Terminate Services
- Report unlawful activity to appropriate regulatory or law enforcement authorities

Nothing in this AUP obligates Bright Packet to monitor customer communications except as necessary to protect its network or comply with applicable law.

8. Government and Regulatory Requests

Bright Packet may disclose customer information when required by applicable law, court order, subpoena, or lawful request from governmental or regulatory authorities.

9. Changes to this Policy

Bright Packet may modify this AUP from time to time. The most current version will be posted on the Bright Packet website and will become effective upon publication unless otherwise stated.

Continued use of the Services after changes become effective constitutes acceptance of the revised AUP.

10. Contact Information

Questions regarding this Acceptable Use Policy, reports of network abuse, or suspected fraudulent activity may be directed to:

Bright Packet, Inc.

Email: noc@brightpacket.com

Website: <https://www.brightpacket.com>

© 2026 Bright Packet, Inc. All rights reserved.