

Acceptable Use Policy

OpsFusion LLC State of California, United States

Effective Date: July 17, 2026 **URL:** <https://opsfusion.cloud/aup>

This Acceptable Use Policy (“AUP”) governs the use of the OpsFusion on-call and incident alerting platform (the “Service”) and is incorporated into the Terms of Service available at <https://opsfusion.cloud/terms>. By using the Service, you agree to comply with this AUP. Capitalized terms not defined herein have the meanings set forth in the Terms of Service.

1. General Conduct

You agree to use the Service only for lawful purposes and in accordance with these Terms, the AUP, and all applicable laws and regulations. You are responsible for all activity that occurs under your account, including all actions taken by your Authorized Users.

2. Prohibited Activities

You shall not, and shall ensure that your Authorized Users do not, use the Service to:

2.1 Illegal Activities

- Engage in any activity that violates any applicable local, state, national, or international law or regulation
- Facilitate or promote illegal activities, including fraud, money laundering, or trafficking
- Violate any third-party intellectual property rights, trade secrets, or proprietary rights

2.2 Spam and Unsolicited Communications

- Send spam, unsolicited messages, bulk messages, or chain messages to alert recipients
- Send alerts or notifications to individuals who have not consented to receive them
- Use the Service for marketing, advertising, or promotional purposes unrelated to on-call alerting
- Manipulate alert content or configurations to send deceptive or misleading messages

2.3 Harassment and Harmful Content

- Harass, threaten, intimidate, stalk, or abuse any individual
- Transmit content that is defamatory, obscene, hateful, discriminatory, or promotes violence
- Impersonate any person or entity, or falsely represent your affiliation with any person or entity
- Transmit content that exploits minors in any way

2.4 Security and Infrastructure

- Attempt to gain unauthorized access to the Service, other accounts, computer systems, or networks connected to the Service
- Circumvent, disable, or interfere with security features, authentication mechanisms, rate limits, or usage quotas
- Introduce viruses, worms, Trojan horses, malware, ransomware, or other harmful code
- Conduct port scans, vulnerability assessments, or penetration tests against the Service without prior written authorization
- Launch denial-of-service attacks or otherwise attempt to overwhelm the Service's infrastructure
- Reverse engineer, decompile, disassemble, or derive source code from the Service
- Scrape, crawl, or use automated means to extract data from the Service beyond authorized API usage

2.5 System Abuse

- Exceed plan-based usage limits through technical manipulation or circumvention
- Create multiple accounts to evade usage limits, suspensions, or bans
- Use the Service in a manner that degrades performance for other customers
- Abuse API rate limits or make excessive, unnecessary, or redundant API calls
- Store data unrelated to on-call scheduling and alerting in the Service
- Use the Service as a general-purpose messaging, communication, or data storage platform

3. Telecommunications Compliance

3.1 SMS and Voice Call Compliance

When using the Service to deliver alerts via SMS or voice calls, you shall comply with all applicable telecommunications laws and regulations, including but not limited to:

- **Telephone Consumer Protection Act (TCPA):** Obtain proper consent from recipients before sending SMS or making voice calls through the Service. Maintain records of consent for each recipient.
- **CAN-SPAM Act:** Ensure that email notifications comply with applicable anti-spam legislation, including providing accurate sender information and honoring opt-out requests.
- **Applicable state and international laws:** Comply with all state-level telemarketing laws and international telecommunications regulations applicable to your use.

3.2 Recipient Consent

You are solely responsible for:

- Obtaining and maintaining valid consent from each individual who receives alerts or notifications through the Service
- Maintaining an up-to-date list of individuals who have opted out of or revoked consent for receiving communications
- Ensuring that communications are sent only to individuals who have a legitimate need to receive them in connection with your on-call scheduling and alerting operations
- Promptly removing individuals who request to stop receiving communications

3.3 Content Responsibility

You are solely responsible for the content of all alerts, notifications, and messages sent through the Service, including:

- Alert titles, descriptions, and metadata
- Custom notification templates and messages
- Any information included in escalation or routing configurations

OpsFusion does not review, screen, or approve alert content. You represent and warrant that your alert content does not violate any applicable law, regulation, or third-party right.

4. Resource and Capacity Limits

4.1 Fair Use

The Service is designed for on-call scheduling and incident alerting. You agree to use the Service within the scope of its intended purpose and within the capacity limits of your subscription plan.

4.2 API Usage

API access is subject to rate limits as documented in our API documentation. You shall not: (a) exceed documented rate limits; (b) use API access to build a competing product; (c) redistribute or resell API access; or (d) use API access for purposes unrelated to your use of the Service.

5. Monitoring and Enforcement

5.1 Right to Monitor

OpsFusion reserves the right to monitor the use of the Service to ensure compliance with this AUP. Monitoring may include reviewing usage patterns, alert volumes, API call patterns, and notification delivery metrics. OpsFusion will not access the content of Customer Data except as necessary to provide the Service, investigate violations, or comply with legal obligations.

5.2 Violation Response

If OpsFusion determines, in its reasonable discretion, that a violation of this AUP has occurred, OpsFusion may take one or more of the following actions:

- **Warning:** Issue a written warning identifying the violation and requesting corrective action
- **Restriction:** Temporarily restrict specific features or capabilities
- **Suspension:** Suspend access to the Service, in whole or in part
- **Termination:** Terminate the account in accordance with the Terms of Service

5.3 Severity-Based Response

- **Minor violations** (e.g., accidental rate limit abuse): Warning with opportunity to cure within a reasonable timeframe
- **Serious violations** (e.g., sending unsolicited communications, TCPA non-compliance): Immediate suspension pending investigation, with notice provided as soon as practicable
- **Critical violations** (e.g., illegal activity, security attacks, malware distribution): Immediate termination without prior notice

5.4 No Refunds

No refund or credit will be issued for any period of suspension or termination resulting from an AUP violation.

6. Reporting Violations

If you become aware of any violation of this AUP, please report it to support@opsfusion.cloud. Include relevant details such as the nature of the violation, affected parties, and any supporting evidence.

7. Cooperation with Law Enforcement

OpsFusion may cooperate with law enforcement authorities and comply with court orders or legal processes that require the disclosure of account information or activity data, in accordance with our Privacy Policy and applicable law.

8. Indemnification

You agree to indemnify and hold harmless OpsFusion from and against any and all claims, damages, losses, liabilities, costs, and expenses (including reasonable attorneys' fees) arising from or related to your violation of this AUP or your Authorized Users' violation of this AUP.

9. Changes to This Policy

OpsFusion may update this AUP at any time. Material changes will be communicated to customers via email or through the Service at least thirty (30) days before they take effect. Continued use of the Service after the effective date constitutes acceptance of the updated AUP.

10. Contact Information

For questions about this Acceptable Use Policy, please contact us at:

OpsFusion LLC Email: support@opsfusion.cloud Website: <https://opsfusion.cloud>

This Acceptable Use Policy was last updated on July 17, 2026.