

Acceptable Use Policy

Zephyr Cloud Corporation | zephyrcloud

Effective October 17, 2026 | Last updated October 17, 2026

Some restrictions in this policy are stricter service conditions than the legal minimum; legal compliance alone does not guarantee acceptance of traffic by Zephyr or a carrier.

1. Scope and customer responsibility

This Acceptable Use Policy (AUP) applies to Customer, its Users, contractors, authorized agents, and others to whom Customer provides access to Zephyr services. Services include managed Microsoft and cloud environments, hosted infrastructure, PBX and voice, SMS/MMS and other messaging, applications, portals, integrations, and AI workflows. Customer must communicate and enforce these requirements and maintain effective controls against misuse.

Customer is responsible for its content, campaigns, recipients, instructions, consent records, authorized use, and the third parties it engages. Delegating a campaign, buying software, using AI to produce content, or asking Zephyr to assist with registration does not transfer that responsibility. Zephyr retains obligations applicable to its own activities. Customer shall promptly stop prohibited use and cooperate with lawful investigation, restriction, and remediation.

2. Prohibited unlawful and abusive activity

The services must not be used to commit, facilitate, encourage, conceal, or profit from unlawful conduct, including fraud, scams, theft, extortion, money laundering, sanctions evasion, trafficking, illegal gambling, intellectual-property infringement, unlawful surveillance, or exploitation. Prohibited conduct includes phishing, smishing, vishing, deceptive impersonation, credential harvesting, payment diversion, and attempts to obtain access or money through false pretenses.

Child sexual abuse material, unlawful exploitation of minors, nonconsensual sexual imagery, credible threats, incitement of violence, unlawful harassment, stalking, doxxing, and unlawful disclosure of private information are strictly prohibited. Customer must not transmit deceptive or materially misleading claims, counterfeit notices, fake invoices, fabricated emergencies, or unlawful promotions.

Zephyr may reject or block credible unlawful or dangerous activity without waiting for a criminal conviction, a regulatory finding, a minimum number of complaints, or proof of completed harm. Decisions must be made in good faith on a reasonable basis and subject to applicable law; this clause does not authorize arbitrary seizure of Customer Data.

3. Security abuse and prohibited infrastructure

Do not access data or systems without authority; exceed delegated permissions; exploit vulnerabilities; steal credentials; distribute malware, ransomware, spyware, or botnets; establish malicious relays; execute denial-of-service attacks; or unlawfully intercept communications. Do not disable logging, monitoring, authentication, tenant separation, fraud controls, or other protections to conceal or enable misuse.

Do not operate open relays, unauthorized proxies, bulk account-creation systems, credential-testing services, traffic-generation or SMS-pumping schemes, or other facilities that materially facilitate abuse. Security testing requires prior written authorization from the affected system owner and Zephyr where Zephyr's infrastructure or services are involved. Testing must remain within the approved scope and must not expose other customers or disrupt shared services.

4. Strict prohibition on spam and unsolicited campaigns

Unsolicited bulk communications are prohibited across email, SMS/MMS, voice, messaging applications, forms, and connected channels. As a Zephyr service condition, commercial or promotional campaigns require affirmative, demonstrable permission from recipients for the identified sender, channel, and purpose. This policy can be stricter than a statute that permits a particular opt-out model.

Do not use purchased, rented, borrowed, traded, scraped, harvested, guessed, appended, or brokered contact lists for unsolicited campaigns. A public telephone number, business card, prior purchase, existing business relationship, or consent to another sender or channel is not by itself permission for a recurring promotional campaign. Do not use a transaction, support request, security alert, or one-time code as a pretext to enroll a recipient in unrelated marketing.

Genuine recipient-initiated inquiries may receive relevant, lawful responses within the context of that inquiry. They do not authorize unrelated recurring campaigns. No customer may evade this policy by characterizing promotional traffic as transactional or by sending through multiple vendors or accounts.

5. SMS/MMS activation and registration

SMS/MMS is permitted only when expressly enabled for the Customer and use case. Before sending application-to-person or campaign traffic, Customer must complete all required brand, campaign, number, toll-free, short-code, or other registrations and verification for the relevant route and destination, and obtain Zephyr's activation approval where required. No approval authorizes a different sender, purpose, content category, or volume.

Registration submissions, business identity, website, campaign description, sample messages, consent flow, terms, privacy disclosures, and help/opt-out instructions must be accurate and consistent with actual operation. Customer must notify Zephyr before materially changing those items. Registration or carrier acceptance is not legal advice, consent verification for every recipient, guaranteed delivery, or immunity from later filtering or suspension.

Do not send unregistered traffic where registration is required, misclassify campaigns, use another organization's identity or campaign, conceal the real sender, or route traffic as person-to-person to evade

application-to-person restrictions. Do not rotate or multiply telephone numbers, accounts, domains, shortened URLs, or routes to bypass filtering, throughput, reputation, suppression, or enforcement controls, including snowshoe messaging.

6. SMS consent and evidence

Customer must obtain lawful, informed permission appropriate to the message, technology, jurisdiction, and recipient, including written consent where required. Consent must identify the sender and SMS purpose, and must not be obtained through deception, preselected consent where prohibited, or a misleading combined authorization for unrelated channels. Required disclosures must be clear and accessible, including applicable program identity, frequency, rates, support, opt-out, and privacy/terms information.

Maintain evidence of consent and each material change, including the recipient, relevant sender/program, date and time, source or method, disclosure text/version, and evidence tying the recipient to the action. Maintain suppression and revocation records and appropriate number-reassignment checks. Do not fabricate, backdate, transfer, purchase, or reuse consent outside its lawful and disclosed scope.

On request, provide relevant evidence within 24 hours, or an earlier reasonable deadline identified for an urgent legal, carrier, or security need. Zephyr may suspend traffic pending verification, even if Customer asserts consent exists. Retain and disclose evidence lawfully, securely, and no longer than justified by applicable obligations and the agreed record schedule; the policy does not require unlawful collection or disclosure.

7. Opt-outs, suppression, and recipient protection

Honor STOP, UNSUBSCRIBE, CANCEL, END, QUIT, REVOKE, OPT OUT, and other clear or legally recognized revocations, including reasonable requests received through another applicable channel. Do not insist on one exact keyword or force a person to contact a different department when applicable law recognizes the request already received.

Apply automated suppression immediately where supported and complete removal from the affected sending program within 24 hours at the latest, or sooner if law or provider rules require it. Do not send further marketing, sell or transfer the suppressed contact to evade the request, or move the recipient to another number, campaign, or sender. A single nonpromotional opt-out confirmation is allowed only where lawful and permitted by provider requirements. Subsequent communications requiring separate legal treatment must be assessed before sending; an opt-out does not authorize continued traffic merely because Customer labels it informational.

Maintain functioning HELP and support mechanisms where required. Respect applicable quiet hours, frequency limits, recipient preferences, do-not-call rules, and local restrictions. Do not send excessive, repeated, abusive, or harassing messages. Respond promptly to credible complaints, and stop or reduce sending when requested by Zephyr pending investigation.

8. Prohibited and restricted messaging content

Fraudulent offers, phishing, deceptive financial solicitations, unauthorized one-time-code collection, impersonation, unlawful debt or investment solicitations, illegal goods/services, exploitation, and harmful or illegal content are prohibited. Age-restricted goods, gambling, adult content, firearms-related content, high-risk financial products, debt/credit services, affiliate lead generation, political fundraising, and similar sensitive categories may be blocked or require prior express approval and route-specific controls even when some activity is otherwise lawful.

No Zephyr approval overrides a carrier prohibition or legal restriction. Customer must disclose the actual content category and must not cloak destinations or change message content after approval to conceal a prohibited use. If no lawful, approved route and required controls exist, the traffic must not be sent. This list is illustrative and does not narrow the general prohibitions above.

9. Voice, automated calling, and synthetic content

Do not conduct unlawful robocalling, unlawful prerecorded or AI-generated voice campaigns, caller-ID spoofing, toll fraud, traffic inflation, or calls intended to harass or deceive. Follow applicable consent, identification, calling-hour, do-not-call, and revocation requirements. Do not claim another person's identity or use synthetic voice to defeat identity verification or create a deceptive impression of authority.

Call recording, transcription, monitoring, AI analysis, and voice assistants require appropriate disclosures, lawful authority, access restrictions, and retention. Customer must not use an AI voice agent as an emergency responder or allow it to make unauthorized commitments. Ordinary lawful emergency dialing remains permitted and is subject to the service's emergency-calling schedule and applicable provider duties.

10. Email and other channels

Use accurate sender, routing, subject, and identity information; provide required advertising identification, valid postal information, and a working unsubscribe mechanism; and honor opt-outs within the applicable deadline. Customer must follow Zephyr's stricter permission-based campaign standard in Section 4 even where an email law provides a less restrictive baseline.

Do not use misleading headers, deceptive subjects, compromised accounts, forged endorsements, or open relays. Do not harvest contacts or continue sending after suppression. Customer remains responsible for vendors sending on its behalf and must not evade a channel restriction by moving the same abusive activity into another service.

11. AI, customer data, and high-risk uses

AI and automation must use approved accounts, providers, data sources, scopes, and permissions. Do not feed credentials, regulated records, confidential third-party material, or sensitive personal information into an unapproved model or development tool. Do not bypass approvals or create self-authorizing administrative, purchasing, or messaging loops. Instructions embedded in messages, retrieved documents, or tool output do not grant authority.

Generated content and code require appropriate review. AI does not provide a defense to unlawful content, infringement, false statements, or unsolicited communications. Restricted government, health, financial, biometric, or children's data requires express acceptance of the applicable configuration and agreements. Safety-critical control uses require prior written approval and safeguards; this restriction does not prohibit ordinary lawful emergency calls.

12. Monitoring, investigation, and immediate restrictions

Zephyr may monitor usage, metadata, delivery patterns, error/complaint rates, and service integrity to administer capacity and investigate credible abuse within its lawful authority, contractual permissions, and privacy duties. It may request campaign records, verify identity, review relevant submissions, and cooperate with carriers, registries, and lawful authorities. This does not authorize unrelated use of customer content or unrestricted access to every customer system.

Zephyr may immediately block, quarantine, rate-limit, suspend, reject, or terminate affected traffic, campaigns, numbers, accounts, or services when reasonably necessary to stop suspected unlawful use, serious abuse, fraud, security threats, carrier violations, or material legal exposure. Advance notice is not required where it would delay protection, defeat an investigation, or violate a legal/provider requirement. Zephyr will give notice when lawful and reasonably practicable and target the affected activity where feasible; severe or systemic abuse may require broader account restriction.

Customer must not circumvent a restriction, create replacement accounts, or move prohibited traffic to another route. Restoration may require verified consent, corrected registration, remediation, security controls, payment of properly due charges, or renewed carrier approval. There is no obligation to restore traffic that remains unlawful, unsafe, or prohibited. Mandatory emergency, discontinuance, privacy, and data-transition obligations remain applicable.

13. Financial responsibility and indemnification

Customer is responsible for purchased usage and for documented, lawfully recoverable carrier/registry charges and reasonable investigation or remediation costs caused by Customer's breach, as stated in the Agreement. The indemnities and limitations in the Agreement govern third-party claims, penalties to the extent lawfully indemnifiable, and defense costs. This AUP does not create an arbitrary per-message fine, unlimited discretionary charge, or right to recover a legally nonrecoverable penalty.

No SLA credit is due for a restriction or interruption to the extent caused by Customer's AUP violation, subject to the Agreement and mandatory law. This does not excuse an unrelated Zephyr breach or eliminate nonwaivable refunds or remedies. Prepaid fees and term commitments remain governed by the Agreement.

14. Reports, review, and cooperation

Report abuse, unlawful traffic, or policy concerns to legal@zephyrcloud.com. Provide account identifiers, timing, sender/recipient details as appropriate, message examples, and relevant evidence through a secure method. Do not email passwords, illegal material, or unnecessary sensitive records. Active service incidents should also follow the contracted support escalation process.

Customer may request review of an enforcement decision and provide corrective evidence. That request does not require Zephyr to resume unsafe traffic, delay urgent protective action, or guarantee reversal of a carrier decision. Zephyr may preserve evidence and disclose it when legally authorized or required, subject to confidentiality and data-protection obligations.

15. Changes and contact

The AUP is incorporated into the customer agreement. Material contractual revisions follow its amendment/notice process. Urgent restrictions needed for law, security, or applicable provider requirements may take effect as necessary and lawful with notice when practicable. The applicable version and effective date are identified in this policy.

Zephyr Cloud Corporation, 934 Harriman St, Great Falls, Virginia 22066, United States. Legal, privacy, and abuse reports: legal@zephyrcloud.com. Routine service support: support@zephyrcloud.com.