FLIGHT MOBILE ACCEPTABLE USE POLICY

Effective February 1, 2026

By subscribing to the mobile voice, messaging and data services ("Flight Mobile" or the "Service") of Orbitel Communications LLC ("Company"), you agree not to use the Service for any unlawful purpose and to comply with all terms and conditions of this Flight Mobile Acceptable Use Policy (the "Policy"). Company posts the current version of this Policy on the its website and may change it from time to time without notice to you by posting updated versions at this website or another website about which you have been notified. You and other users associated with your Flight Mobile account should periodically review this Policy in order to conform to the most recent version. Revisions are effective immediately upon posting. This Policy, as it may be changed and updated over time, is incorporated into your Flight Mobile Subscriber Agreement. If you, or any other users on additional lines associated with your Flight Mobile account, fail to abide by any of the terms of this Policy, Company may suspend or terminate the provision of the Service to you or any additional users, as further detailed below in the paragraph entitled "Violation of this Policy." Additionally, Company reserves the right to charge you for any direct or indirect costs Company may incur in connection with your failure to abide by this Policy. Your data use on Flight Mobile will also be subject to the Company's Internet Acceptable Use Policy which may be found at https://www.orbitelcom.com/legal/Flight-Mobile-Acceptable-Use-Policy.pdf and is incorporated herein by this reference.

USE BY MULTIPLE USERS AND DEVICES. Flight Mobile shall be used only by you, and if you have multiple lines associated with your Flight Mobile account, users of those other lines; and use of the Flight Mobile service is subject to your and any such other users' compliance with this Policy. You shall have sole responsibility for ensuring that all users of your Flight Mobile account understand and comply with the terms and conditions of this Policy. You are legally and financially responsible for any misuse of the Service, even if the inappropriate activity was committed by users of other lines associated with your Flight Mobile account or on devices of third parties connected to your Flight Mobile account, a friend, family member, guest, employee, or any other person with access to the Service through your account. Therefore, you must take steps to ensure that others do not gain unauthorized access to the Service, for instance by strictly maintaining the confidentiality of your passwords or by appropriately protecting physical access to the devices you use in connection with the Service. You are solely responsible for the security of any device you choose to connect to the Service, including any data stored on that device. Company recommends against enabling file sharing (e.g. Airdrop) of any sort.

UNLAWFUL USE AND PROHIBITED ACTIVITIES. Flight Mobile may be used only for lawful purposes. You will not use or allow others to use the Service in any manner that is in violation of any applicable federal, state, local or international laws or regulations or to promote, engage in, or enable illegal activity or conduct that violates or infringes upon the rights of any person. Transmission or distribution of any material in violation of any applicable law or regulation is prohibited, including, without limitation, material protected by copyright, trademark, trade secret, or other intellectual property right used without proper authorization, and material that is obscene, illegal, defamatory, constitutes an illegal threat, or violates export control laws.

Flight Mobile is not intended to be used in any manner which has any of the following effects and such use is prohibited if it: (a) compromises network security or capacity; (b) excessively and disproportionately

contributes to network congestion; (c) adversely impacts network service levels or legitimate data flows; (d) degrades network performance or causes harm to the network or other customers; (e) is sold, resold, assigned, shared, licensed or otherwise provided to or utilized either alone or as part of any good or service; (f) tampers with, reprograms, alters or otherwise modifies a mobile device to circumvent any of Company's policies or violate anyone's intellectual property rights; or (g) defeats, obstructs, or penetrates, or attempts to defeat, obstruct or penetrate the security measures of the mobile network or systems, another entity's network or systems, or the accounts of others.

Flight Mobile is intended for typical consumer use and is not intended for any purpose other than personal and non-commercial residential use. Some examples of prohibited uses are:

• *Prohibited Voice Uses*

- Use of auto-dialers
- Telemarketing, advertising or commercial solicitation to a person
- Extensive call forwarding or use of call forwarding or conferencing features to act as a bridge to chat lines or other conferencing facilities.
- Operating a call center or conference line
- Usage for monitoring services, data transmissions, or transcription services
- Transmissions or reception of broadcasts over teleconferencing facilities or other means
- Transmissions or reception of recorded material (other than your recorded consumer voice messages)
- Transmission or reception of communications which do not consist of consumer voice messages or
- Transmission or reception of communications which do not consist of standard voice calling involving live dialogue between individuals.

• *Prohibited Message Uses*

- Transmission or reception of communications which do not consist of consumer or SMS messages.
- Resale to others
- Bulk messaging such as “blast” or other mass messaging, including commercial messaging, also known as “spam.”
- Transmission of automatically generated messages, or
- Engaging in activities that may generate payments to a customer due to the customer’s use of Flight Mobile.

• *Prohibited Data Uses*

- Hindering other customers’ access to the wireless network
- Compromising network security or capacity
- Excessively and/or disproportionately contributing to network congestion
- Excessively and/or disproportionately using data roaming capabilities on roaming partner networks
- Usage that has an adverse impact on network service levels or legitimate data flows
- Usage that degrades network performance
- Usage that causes harm to the network or other customers
- Reselling data services, either alone or as part of another good or service
- Tethering a wireless device to a computing device without having a subscription to a service plan designed to allow such usage
- A particular use for which a service plan or feature is offered, but to which you have not subscribed

- Obscuring, masking, altering, or changing IP address to a different address than that assigned by the network carrier, or
- Activating a device on a service plan not intended for its use (e.g., activating a 4G device on a service plan intended for 4G LTE devices).

VIOLATION OF THIS POLICY. Company prefers to advise customers of inappropriate behavior and any necessary corrective action. However, if the Service is used in a way that Company or its suppliers, in their sole discretion, have a reason to believe violates this Policy, Company or its suppliers may take any responsive actions they deem appropriate.

When an account shows excessive call volumes or abnormal messaging or data usage compared to a typical, non-commercial, residential user, Company may review the calling, messaging and/or data patterns further. Company and its suppliers reserve the right at any time to review communication traffic patterns and volumes to identify, and take remedial action in response to (including imposing additional fees or Service termination), the following, among other things:

- Relative proportion of in-state, out-of-state, or international calling destinations
- Excessive calls to the same destination telephone number, indicative of an automated call forwarding device or of chat line or conference bridge usage
- Excessive inbound calls
- Excessive calls made during business hours
- Excessive short-duration outbound calls made during business hours
- Excessively long calls to any single number
- Excessive calls made during a month
- Calls made to numerically consecutive numbers, indicative of autodialing or "robocalling"
- A high volume of calls terminated and re-initiated consecutively, which in the aggregate result in excessive call lengths during a specific time frame
- Excessive inbound text messages
- Excessive outbound text messages, or
- Other unusual or atypical calling or usage patterns indicative of an attempt to evade Company's enforcement of this Policy.

Company does not monitor the voice or messaging conversations of its customers in order to enforce this Policy except as necessary to comply with applicable laws (e.g., a lawful subpoena).

If the review of calling, messaging or data usage reveals patterns indicative of use that is inconsistent with a purpose other than personal and non-commercial residential use, then Company may enforce this Policy by taking one or more of the actions described below.

ENFORCEMENT. Company reserves the right to take the following actions for violations of this Policy: temporary or permanent removal of content, cancellation of newsgroup posts, filtering of mobile transmissions and/or the immediate suspension or termination of all or any portion of the Service.

Neither Company nor its affiliates, suppliers, or agents will have any liability for any of these actions. The above-described actions are not Company's exclusive remedies and Company may take any other legal or technical action it deems appropriate.

Company reserves the right to investigate suspected violations of this Policy, including the gathering of information from the subscribers or users involved and the complaining party, if any, and examination of material on Company's servers and network and those of Company's suppliers used in delivering service. During an investigation, Company may suspend the account or accounts involved and/or remove or block

material that potentially violates this Policy. You hereby authorize Company and its suppliers to cooperate with (i) law enforcement authorities in the investigation of a suspected legal violation and (ii) system administrators at other mobile broadband internet access service providers or other network or computing facilities in order to enforce this Policy. This cooperation may include Company providing information about you to law enforcement or system administrators, including, but not limited to, username, subscriber name, IP address, and other account information. Upon termination of your account, Company is authorized to delete any files, programs, and email messages associated with your account. The failure of Company or its suppliers to enforce this Policy, for whatever reason, shall not be construed as a waiver of any right to do so at any time. You agree that if any portion of this Policy is held invalid or unenforceable, that portion will be construed consistent with applicable law as nearly as possible, and the remaining portions will remain in full force and effect.