

## Fair & Acceptable Use Policy (FAUP)

No filtering or blocking of specific types of traffic is applied, but the nextGen Broadbeam service is subject to the following Fair & Acceptable Use Policy (FAUP) that assures a responsible network usage. The nextGen Broadbeam service is entirely **flat-fee** and there are **no** limits with respect to the amount of traffic.

The FAUP specifies the actions prohibited by OmniAccess to Clients of the BroadBEAM VSAT network. The primary purpose of this FAUP is prevent the illegal use of the BroadBEAM VSAT services as defined in Spanish law or the inappropriate use or misuse of the Services on the basis of OmniAccess's own judgment and discretion. This FAUP further defines the rights that OmniAccess has to ensure consistent and acceptable use of the BroadBEAM VSAT Services and the network by all users, as well as safeguard and protect its own commercial interests. OmniAccess reserves the right to modify this FAUP at any time. Changes made to the FAUP become effective upon posting of the modified FAUP at the company-website <http://www.omniaccess.com/faup>. It is the user's responsibility to ensure their awareness of any such changes. OmniAccess reserves the right to suspend or terminate the User's service immediately and without prior notice, if the Client is in breach of any aspect of the FAUP whereby OmniAccess will not be liable for any damages and/or refunds whatsoever (either direct or consequential) due to the loss of service in such cases. OmniAccess will promptly inform the Client of any decisions to suspend or otherwise limit the service to the Client.

Under the terms of the FAUP, the nextGen Broadbeam service may be freely used with the exception of usage that falls in one or more of the following categories:

- **Illegal use.** The VSAT network operated by OmniAccess may be used only for lawful purposes. Transmission, distribution or storage of any material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret or intellectual property rights used without proper authorization, and material that is obscene, defamatory, constitutes an illegal threat, or violates export control laws.
- **Sharing & Commercial Use.** The Client is prohibited from reselling or sharing (parts of) the nextGen Broadbeam services in any way with users which are not physically located on the vessel that belongs to the Client listed in **Section 1** ("Client Details") of this nextGen Broadbeam Service Agreement .
- **Non-compliance with local regulations regarding the use of VSAT equipment.** Clients agree that it is their sole responsibility to make sure their on-board VSAT equipment at all time meets all regulations imposed by both the flag-state of the vessel as well as the country in whose territorial waters the equipment is operated. OmniAccess will co-operate with any legitimate request made by the competent authorities to restrict or disable the usage of the nextGen Broadbeam service if local regulations so dictate. OmniAccess will not be liable for any damages and/or refunds whatsoever (either direct or consequential) due to the loss of service in such cases, or for any fines the competent authorities may impose on the Client as a result of the foresaid non-compliance.
- **Disruptive use.** The nextGen Broadbeam service has been designed with professional usage in mind and allows the Client to transfer large amounts of data (like watching streaming video-content online). OmniAccess does not enforce any generic usage limits on any nextGen Broadbeam service package: Clients can download and upload as much as they like every month. But if the Client uses the service in an excessive manner – like continually downloading large files, engaging in "Peer to Peer" file-sharing activities or disruptive traffic generated by computer viruses – then OmniAccess reserves the right to request Clients to lower their data-usage. In exceptional circumstances (and only after prior notification), OmniAccess may decide to rate-limit or block any traffic-type OmniAccess consider to be disruptive in case the Client fails (or is unable) to remedy the cause of the excessive traffic. Any such limitation shall not exceed the limit of the contracted **CIR** (as indicated in **Section 2**).
- **Violations of system and network security.** Violations of system or network security are prohibited, and may result in criminal and/or civil liability. OmniAccess will investigate incidents involving such violations and will involve and will co-operate with law enforcement if a criminal violation is suspected. Examples of system or network security violations include, without limitation, the following:
  - Unauthorized access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without the express authorization of the owner of the system or network;
  - Unauthorized monitoring of data or Traffic on any network or system without the express authorization of the owner of the system or network;
  - Interference with service to any User, host or network including, without limitation, DDOS, mail-bombing, flooding, deliberate attempts to overload a system and broadcast attacks;
  - Forging of any IP packet header or any part of the header information in an email or a newsgroup posting.

If approached with complaints relating to any system or network security violations, OmniAccess will co-operate and assist the Police and law enforcing bodies with their investigations in order to bring such abuse and violations to an end.

- **Illicit E-mails.** It is explicitly prohibited to send unsolicited bulk e-mail messages ("junk mail" or "spam") of any kind (commercial advertising, political tracts, announcements) etc. It is also explicitly prohibited to allow others to send unsolicited bulk e-mail messages or viruses either directly or by relaying through the Client's systems. For the avoidance of doubt, Clients must ensure that their systems cannot be relayed through. Users may not forward or propagate chain letters nor malicious e-mail. A Client may not solicit e-mail for any other address other than that of the Client, except with full consent of the owner of the referred address.
- **Interference.** The client is required to make sure at all times that the transmission equipment (including the stabilized platform) aboard the vessel does not cause any (intentional or unintended) interference to any other users on the VSAT network. If OmniAccess detects any transmissions that cause interference, the Client will be informed immediately and agrees to carry out any action that OmniAccess may deem necessary to halt the transmission of the interference. Failure to comply with this obligation will grant OmniAccess the right to terminate, suspend or limit the service with immediate effect, without notice, and shall indemnify OmniAccess against liability for any damages or other forms of compensation that could be claimed by the client. In the event the interference is causing service interruptions to other network users, OmniAccess may hold the client that caused the interference responsible for any damages and/or claims that may result from these service outages.