



Business Satellite Solutions

GALILEO USE POLICY

This Acceptable Use Policy is intended to help enhance the use of the Internet and the Ground Control Systems Galileo/Tachyon Network by preventing unacceptable uses and setting forth the actions prohibited to users of the Ground Control Network. Violation of this Policy may result in the suspension or termination of your access to Communications Services.

Illegal Use

Ground Control Services shall only be utilized for lawful purposes. Transmission, distribution or storage of material in violation of any applicable law or regulation is strictly prohibited. Examples of such violations include, but are not limited to, material protected by copyright, trademark, trade secret or other intellectual property rights adopted without proper authorization, material that is obscene or defamatory, material that constitutes an illegal threat, or violation of laws regulating export control.

Intended Use

Ground Control Services are designed for end user Internet access including email and web browsing. Ground Control Services are not to be used for network infrastructure applications or media intensive content. Ground Control reserves the right to limit or deny access for applications including, but not limited to:

- Web hosting
- Streaming services
- Backbone connectivity
- Internet POP connectivity
- Peer to peer file sharing (serving)
- Constant bit rate services

* Should end user consume or utilize more bandwidth than the bandwidth package subscribed to permits, there will be additional throughput charges.

Ground Control reserves the right to limit or deny access to traffic generated by malicious applications including but not limited to:

- Computer or network viruses
- Trojan horses
- Denial of Service attacks

SECURITY

Breach of system or network security is prohibited and may result in criminal action or civil liability. Investigation by Ground Control of suspected violations may involve law enforcement agencies depending on whether the violation is deemed to be criminal. Types of system or network security violations include, without limitation, the follows:

- Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner of the system or network.
- Interference with service to any user, host or network including, without limitation, mailbombing, flooding, deliberate attempts to overload a system, or broadcast attacks.
- Forging of any TCP-IP packet header or any part of the header information in an email or a newsgroup posting.
- 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 express authorization of the owner of the system or network.

EMAIL

- Unsolicited email messages are forbidden. These include, without limitation, commercial advertising or informational announcements. Use of another site's mail server to relay mail without the express permission of the site is strictly prohibited.
- Posting the same or similar message to one or more newsgroups (excessive cross-posting or multiple-posting, also known as SPAM) is explicitly prohibited. You may not post or transmit any message, data, image or program which is libelous, defamatory, indecent, obscene or pornographic.
- You may not post or transmit any file which contains viruses, worms, "Trojan Horses" or any other contaminating or destructive features.

INDIRECT OR ATTEMPTED VIOLATIONS OF THIS POLICY AND ACTUAL OR ATTEMPTED VIOLATIONS BY A THIRD PARTY ON BEHALF OF A GROUND CONTROL CUSTOMER OR A CUSTOMER'S END USER, SHALL BE CONSIDERED VIOLATIONS OF THE POLICY BY SUCH CUSTOMER OR END USER.

NOTIFICATION

Notification or complaints regarding illegal use of system or network security, email abuse or SPAM should be sent to: support@groundcontrol.com. or contact the Ground Control Legal Department at (805) 783-4600.