

CapRock Communications Acceptable Use Policy

This ACCEPTABLE USE POLICY (“Policy”) is subject to the definitive agreement governing the provision of telecommunications services (the “Services”) from CapRock Communications (“CapRock”) to the purchaser of the Services (“Customer”), and this Policy governs the use of any Services that enable the Customer to access content via the Internet, either directly or indirectly. Customer’s use of the Services constitutes acceptance of, and agreement to, the terms and conditions of this Policy. CapRock reserves the right to modify this Policy from time to time.

Customer agrees that it will not initiate, participate in, or allow any of the following activities through or in connection with the Services:

- Using the Services for illegal purposes or for the transmission of material that (i) is unlawful, harassing, libelous, defamatory, profane, abusive, threatening, harmful, vulgar, obscene, indecent or sexually explicit; (ii) infringes the intellectual property rights or the contractual, proprietary or fiduciary rights of others (unless with the express written permission of the owner of such right); (iii) violates or is invasive of the privacy or publicity rights of others; (iv) constitutes or encourages conduct that would constitute a criminal offense or would otherwise violate any applicable local, state, national or international law, including without limitation the U.S. export control laws and regulations; or (v) unreasonably interferes with CapRock’s or any underlying carrier’s network or system or the use of such system by other customers;
- Engaging in any activity which threatens the integrity of any computer system, or violates generally accepted standards of Internet conduct and usage, including but not limited to “denial of service” attacks, web page defacement, hacking, port and network scanning, “phishing” or the fraudulent use of email messages that appear to come from legitimate businesses for the purpose of identity theft, unauthorized system penetrations or distributing bugs, viruses, worms, Trojan Horses or such other harmful elements;
- Attempting to break security, or in fact, breaking the security of any computer network, accessing an account which does not belong to Customer, or any other act of a malicious nature which may reasonably result in harm or damage to another user’s service, equipment or privacy, including but not limited to any act of fraud;
- Directly or indirectly sending any spam or unsolicited mass distribution of e-mail;
- Engaging in any of the foregoing activities by using the service of another provider, by channeling such activities through any of CapRock’s IP addresses as a mail drop for responses or otherwise by using the services of another provider for the purpose of facilitating any of the foregoing activities if such use of another party’s service could reasonably be expected to adversely affect the Services; or

- Reselling the Services to any third parties without prior express written consent from CapRock.

Customer acknowledges and agrees that information related to the use of the Services may be required to be provided by CapRock in compliance with any applicable laws, regulations, rules, order and decrees. Without implying any right of Customer to permit a third party to use the Services, Customer agrees that its customers, if any, and end-users (collectively, "End Users") are bound by the terms of this Policy. Customer agrees to notify its End Users of the terms of this Policy and to be responsible for any violation of this Policy by its End Users. Customer further agrees, on behalf of itself and its End Users, to comply with all laws, rules, regulations and policies applicable to any underlying carrier's network or to any server, computer database, hardware or other equipment, software, web site or ISP that is accessed through the Services.

Should Customer or its End Users violate any terms of this Policy, CapRock may take such action as it deems necessary to protect the integrity of its network and resolve any Policy violation, including but not limited to immediately suspending, limiting or terminating Customer's access to the Services without notice, as well as conducting regular system monitoring, port scanning and shutting down of ports affected by viruses, worms or other malicious code, investigating suspected violations of this Policy, instituting action to recover the costs and expenses of identifying offenders and terminating their access to and use of the Services, and levying cancellation charges to cover CapRock's costs in the event of termination of access to the Services. Nothing contained in this Policy shall be construed to limit CapRock's rights or remedies available at law or in equity.