Commercial Internet Acceptable Use Policy

The following section of this Document comprises Frontier Communications' (referred to as Frontier, FrontierNet®, FrontierNet.net, gvni.com, epix.net, Citlink.net, and/or NewNorth.net) "Acceptable Use Policy" (AUP) as it exists the day that this agreement between Frontier and the Customer is entered into. As UCE and "hacking" technology develops at an alarming rate and is expected to continue to do so, Frontier reserves the right to add, remove, or modify specific prohibitions from this section of this Document. The Customer recognizes and agrees that the online AUP prohibitions, to be maintained by Frontier Communications, and always available to all Customers and to the public as the company's web pages supersede the prohibitions listed in this document.

User understands that the following restrictions are applied to the service. If violated, the service will be terminated without notice:

Customer shall not do any of the following, or permit any third party under its control (including its customers and their authorized users [ad infinium]) to do the following, and must include provisions in its service agreements for its customers and authorized users that restrict them from doing any of the following:

1. Restrict or inhibit any other user from using and enjoying the Service and/or the Internet.
2. Upload, post, publish, transmit, reproduce, distribute, or participate in the transfer or sale, or in any way exploit any information, software or other material obtained through the Internet which is PROTECTED BY COPYRIGHT or other proprietary rights or derivative works with respect thereto, without obtaining permission of the copyright owner or rightholder. Repeated copyright infringements are grounds for termination of service.
3. Use the SMTP services of a third party for the purposes of relaying or sending electronic mail messages without the express permission of that third party.
4. Host a publicly-accessible "open relay" SMTP or anonymous remailer service for any purpose, cause, or reason.
5. Post a commercial advertisement to any USENET newsgroup, Internet "chat room", bulletin board, or similar forum, if the target forum is not specifically chartered for public advertisement by non-private parties of items "for sale".
6. Post to any USENET Newsgroup or other newsgroups, forum, email mailing list or similar group or list articles which are offtopic according to the charter or other public statement of the group.
7. Send Unsolicited Commercial Email (UCE, also known as SPAM) to any number of email users or lists.
8. Maintain, or send email to, "opt-in targeted marketing lists" if the Customer cannot demonstrate, to the satisfaction of Frontier, that the members of the list(s) Frontier.com

2 have knowingly requested to be added to the list(s) in question through direct action of their own doing, and that easily-accessible, automated opt-out/removal mechanisms are in place and available to the members of the list(s).

9. Engage in any activity that is, or appears to be, an attempt to gain unauthorized access to a remote system or network, or to gain information that could later be used to assist in gaining unauthorized access to a remote system or network, such as port scanning, dictionary attacks, Denial of Service attacks, server/service hijacking, etc.
10. Engage in any of the foregoing activities using the service of another provider, but channeling such activities through an Frontier account or remailer, or using an Frontier account as a mail drop for responses to UCE, or hosting a web site that is advertised via UCE that originates from a non-Frontier connected source, or otherwise requiring return transit through the Frontier Internet backbone.
11. Falsify or "spoof" user information provided to Frontier or to other users of the Service, and for handling all complaints and trouble reports made by its own customers and authorized users.
12. Use the Service in violation or contravention of the Communications Act of 1934, as amended by the Telecommunications Act of 1996, or any other applicable law, regulation, order or other governmental directive, or abuse or fraudulently use the Service in any way not specifically set forth above.
13. Advertise, transmit, or otherwise make available any software, program, product, or service that is designed to violate this AUP, which includes but is not limited to, the facilitating the sending of Unsolicited Commercial Email (UCE also known as SPAM). Further, if Customer is notified by a Frontier Abuse Response Team member through any form of communication, or the Customer discovers on their own or through any other means, that the Customer themselves or any third party under his/her control (including his/her customers and their authorized users [ad infinium]) of a violation of any of the foregoing prohibitions, the Customer will take whatever steps are necessary to stop such activity, and prevent repeat violations by the offending entity.
14. Remote Access – Although Frontier encourages its customers to use Remote Access Dialup when traveling, Frontier may suspend or terminate service if such usage exceeds a reasonable amount of usage that would normally be expected from a person occasionally traveling away from home. Remote Access Dialup usage is defined as Internet data calls to local access numbers beyond Frontier's local exchange telephone company territory.

The Customer will respond to all violations reported by the Frontier Abuse Response Team within 1 (one) business day of the violation being reported, and will have put a stop to the activity within 2 (two) business days of the violation first being reported. If a Frontier.com 3 single entity is responsible for multiple violation reports that are sent to the Customer by the Frontier Abuse Response Team, only a single response from the Customer back to the Frontier Abuse Response Team is required, provided that the Customer has taken whatever

action was necessary to stop the current violation and prevent future repeat violations by the offending entity.

If, after the Customer has notified Frontier that the Customer has taken action to prevent future violations by a given entity, that entity is found accessing the Frontier network, Frontier may consider this a breach of its system integrity, and Frontier reserves the right to deal with this situation by whatever legal means deemed appropriate by Frontier.

Customer acknowledges that mounting complaints shall have a negative impact on the business and/or reputation of Frontier. Therefore, notwithstanding anything contained in this Policy or any Service Agreement to the contrary, Frontier may elect, at its sole discretion, to logically suspend any Frontier provided Internet service connection on its network if reports of abuse, UCE, or other activity deemed to have a negative impact on the network exceeds 60 complaints received in any rolling 30 day period. Prior notification of such action is not required but will be provided within 36 hours of a suspension. Service will be re-established upon the provision of satisfactory assurance to Frontier by the Customer that the complaints will not continue to a degree that exceeds the thresholds indicated above.

Complaints regarding the violation of any of the above conditions by any of Frontier's downstream networking clients or their customers, should include notification to the Frontier Security/Abuse Response Team (abuse@frontier.com) in addition to the ISP/NSP the violation actually sourced from.

Any complaints sent to ipadmin@frontier.com or hostmaster@frontier.com as listed in the frontiernet.net whois record, or sent to postmaster@frontier.com and webmaster@frontier.com may be forwarded to the Frontier Security/Abuse Response Team at abuse@frontier.com if the separate groups that answer those addresses have the time to do so. However, complaints sent to any of these addresses will take much longer to process if they are forwarded to the abuse team due to the delays in forwarding, as none of these addresses are valid points-of-contact for abuse complaints.

Abuse complaints to abuse@frontier.com are processed within two (2) working days upon receipt.

Complaints to the Frontier Security/Abuse Response Team should:

1. Be specific as to the nature of the complaint (i.e. UCE, Usenet Spam, etc).
2. Include a copy of the offending message/article with full message or article headers included.
3. Include a trace route or WHOIS output that demonstrates transit through the Frontier backbone to one of the responsible parties; or that they are a networking customer of Frontier or one of Frontier's networking customers.

Those who believe users of our services are infringing their copyrights must submit their complaints in writing to our Designated Agent to Receive Notifications of Claimed Infringement, Mark Nielsen, dmca@frontier.com, Frontier Communications Corporation, 401 Merritt 7, Norwalk, CT 06851, 1.203.614.5600.

CHILD PORNOGRAPHY PROHIBITED

Customers may not use our network in any fashion for the transmission or dissemination of images containing child pornography. Complaints and reports of child pornography may be made to abuse-child@frontier.com . If circumstances indicate that child pornography is apparent, Frontier will report the circumstances to appropriate authorities, including but not limited to subscriber information relating to any person who has uploaded, transmitted, distributed or otherwise promoted the image that is the basis for the complaint. Frontier may without further notice remove, block or cease distribution of the content that is the subject of the complaint.

Last Updated: November 20, 2015