PILOT FIBER

Acceptable Use Policy

Last updated: January 2025

Our Acceptable Use Policy ("AUP") outlines what you can and cannot do when using Pilot's services (the "Services"), and what the responsibilities are of individuals who access the Services.

1. Prohibited uses of Pilot's services

Public Servers and Proxies: Unless permitted in writing, you cannot operate a server or program which makes a Service available to the general public. You also cannot use Pilot's services to host servers or programs on behalf of others in exchange for compensation (i.e. running a web hosting company) without Pilot's prior written consent. Any servers or programs that are to be used solely within your organization are permitted.

Spamming: You cannot send unsolicited bulk and/or commercial messages using our services. In other words, don't spam. If you are sending bulk e-mail of any kind, you must maintain complete and accurate records of both Opt-In and Opt-Out requests. Sending "Opt-Out" only email is strictly prohibited and is considered unsolicited.

Copyright Infringement: You cannot engage in any activity that infringes or misappropriates the intellectual property of others. This includes but is not limited to copyrights, trademarks, service marks, trade secrets, software piracy, and patented content.

Obscene Content: You cannot transmit or distribute any material which violates any applicable law or regulation. Using Pilot's network to advertise, transmit, post, display, or otherwise make available child pornography or obscene material is prohibited. While we will never prohibit any material allowed by law or protected by your First Amendment rights, we are required by law to notify law enforcement agencies when we become aware of the presence of child pornography being transmitted through our network.

Defamatory or Abusive Language: You cannot use our services as a means to transmit or post defamatory, harassing, abusive, or threatening language.

Forging Headers or Content: You cannot forge or misrepresent packet or message headers, whether in whole or in part, to mask the originator of the content. In addition, you cannot forge or misrepresent any data with false or misleading content.

Illegal or Unauthorized Access: Hacking is not allowed. You may not access computers, accounts, or networks belonging to any other party illegally or without authorization. We do not permit the utilization of network scanning utilities unless authorized in advance. You are prohibited from attempting to disrupt, degrade, impair, or otherwise violate the integrity of our services or the computers, accounts, or networks of any other party. You may not engage in any activity that could potentially result in the 'blacklisting' of any Pilot IP addresses.

Technology Exploitation: You cannot attempt to exploit any scripts presented on web pages, or perform any activities that disrupt the use of or otherwise interfere with the ability of others to use our services.

Export Control Violations: You are not permitted to export encryption software over the internet, or otherwise in violation of ITAR to points outside of the USA.

Malicious Activities: You cannot send internet viruses, worms, or trojan horses. In addition, the coordination of denial of service attacks, SYN floods, or mail bombs is expressly prohibited. In a broader context, we prohibit any activities that will interfere with or disrupt how other users can use our services. We also prohibit any activities that can be harmful to or interfere with third party networks, equipment, websites, or applications.

No Phishing or Pharming: Simulating or emulating communications from and/or to a website of a third party for the purpose of collecting identifiable information, authentication credentials, or any other information from a legitimate user is strictly prohibited. Furthermore, using malware or DNS cache poisoning to wrongfully redirect a user to a simulated service is also prohibited.

Any Illegal Activity: You are not permitted to engage in any activities that are determined to be illegal, including but not limited to: advertising, transmitting, pyramid schemes, credit card fraud, and pirating software.

2. Your responsibilities as a user

You are solely responsible for any material that you either access or distribute using our service. You are also solely responsible for maintaining the security and confidentiality of your credentials and network. You agree to immediately notify us of any unauthorized use of your services, breach of security, or should you become aware of any violations to this AUP by any person. Violation of this AUP or applicable laws or regulations may subject you to immediate termination.

3. DMCA Policy

Pilot will respond in a quick and efficient manner to process and investigate all notices of alleged infringement and will take appropriate actions in accordance with the Digital Millennium Copyright

Act ("DMCA") and other applicable laws. Upon receipt of notices complying with the DMCA, we will make reasonable efforts to notify subscribers of alleged copyright violations, and when under our control, we will remove or disable access to any material claimed to be infringing or claimed to be the subject of infringement and will remove or disable access to any reference or linkage to the material or activity claimed to be infringing. We will terminate the services of Subscribers whom are repeat infringers.

Should you believe that copyrighted work has been illegally copied and is accessible via our services in a way that constitutes copyright infringement, you may notify us by providing us with the information required by Section 512(c)(3) of the DMCA (17 USCA 512). Notices of claimed infringement should be sent to:

> Legal Department
> Pilot Fiber, Inc.
> 1115 Broadway, Floor 12
> New York, NY 10010
> Email: copyright@pilotfiber.com

4. Reporting violations

To report a violation of this AUP, contact abuse@pilotfiber.com.