



## Premier Fiber's Acceptable Use Policy

### **PURPOSE:**

This document, Premier Fiber's Acceptable Use Policy ("AUP"), governs the use of Internet related services provided by Premier Fiber. All contractual terms and tariff terms also apply.

### **INTRODUCTION:**

Premier Fiber's Acceptable Use Policy ("AUP") is intended to help enhance the use of the Internet by preventing unacceptable use. It is not a "terms of service" or a billing guideline.

Please refer to your Terms of Service for terms and conditions applicable to your Internet Service. **PLEASE READ THIS POLICY CAREFULLY BEFORE ACCESSING THE SERVICE. BY ACCESSING THE SERVICE, YOU AGREE TO BE BOUND BY THIS POLICY. IF YOU DO NOT WISH TO BE BOUND BY THIS AUP, YOU MAY NOT ACCESS OR USE THE SERVICE.**

This AUP applies to Internet Services ("Services") provided by Premier Fiber. Your use of the Services indicates your acceptance of and agreement to abide by this Acceptable Use Policy. It is designed to help protect the Service, Premier Fiber customers and the Internet community from irresponsible or illegal activities. Premier Fiber may modify this AUP from time to time. In the event of any inconsistency between Premier Fiber Acceptable Use Policy and the terms of any service agreement, this Acceptable Use Policy shall govern and control.

### **GENERAL POLICY**

Violation of this AUP may result in Premier Fiber reserving the right in its sole discretion to deny or restrict your use of the Services, or immediately to suspend or terminate your Services. If the use of your Services by you or anyone using it, in our sole discretion violates your Terms of Service or other Premier Fiber policies, is objectionable or unlawful, interferes with the functioning or use of the internet or Premier Fiber network by Premier Fiber or other Customers or violates the terms of this AUP. Premier Fiber may, but is under no obligation to, provide advance notice of an AUP violation, via Email or otherwise, and request that such violation be immediately corrected prior to taking action.

### **VIOLATION OF THIS ACCEPTABLE USE POLICY:**



This section is used to address actions, content and or practices that are prohibited by law and by rules set forth by the Premier Fiber. Please review the sections below before using Premier Fiber's Services or networks. The restrictions are not negotiable. Not all Services provided by Premier Fiber are listed or mentioned but are bound by this document.

Customers found to engage in activities that Premier Fiber determines, in its sole discretion, are in violation of this AUP will have their accounts terminated. Premier Fiber may refer potential violations of laws to the proper authorities, may cooperate in the investigation of any suspected criminal or civil wrong, and will cooperate with authorities when required to do so by law, subpoena, or when the public safety is at stake. Premier Fiber assumes no obligation to inform subscribers when information has been provided to law enforcement authorities and, in some cases, may be prohibited by law from providing such notice. Premier Fiber reserves the right to act immediately and without notice to suspend or terminate services in response to a court order or other legal requirement that certain conduct be stopped or when Premier Fiber determines, in its sole discretion, that the conduct may:

- Expose Premier Fiber to sanctions, prosecution or civil action
- Cause harm to or interfere with the integrity or normal operations of Premier Fiber's networks or facilities
- Interfere with another person's use of Premier Fiber's services or the Internet including any and all Denial of Service (DoS) attacks
- Damage or disparage the reputation of Premier Fiber or its services
- Otherwise present a risk of harm to Premier Fiber or Premier Fiber's Customers or their employees, officers, directors, agents, etc.

#### **ILLEGAL & PROHIBITED USE:**

This section is used to address actions, content and or practices that are prohibited by law and by rules set forth by the Premier Fiber. Please review the sections below before using Premier Fiber's Services or networks. The restrictions are not negotiable. Not all Services provided by Premier Fiber are listed or mentioned but are bound by this document.

Customers found to engage in activities that Premier Fiber determines, in its sole discretion, are in violation of this AUP will have their accounts terminated. Premier Fiber reserves the right to limit, restrict and/or prohibit Services it provides to customers, as Premier Fiber determines necessary. The restrictions mentioned apply to all Customers unless specifically documented.

Premier Fiber also reserves the right to cooperate with legal authorities and/or affiliated third parties in the investigation of any suspected illegal activity or civil wrong. Activities or use of Services considered by Premier Fiber to be a violation of this AUP are as follows, but are not limited to:

**Abuse of Email Services:** Sending unsolicited mail messages is prohibited, including without limitation:

- Customers are prohibited from sending unsolicited bulk and/or commercial messages over the Internet ('spamming'). This includes receiving replies from unsolicited emails, (i.e., 'Dropbox' accounts) or configuring any email server in such a way that it will accept third party emails for forwarding (i.e., open mail relay). Bulk email may only be sent to recipients who have expressly requested receipt of such email messages through a 'verified opt-in' process. Users that send bulk email messages must maintain complete and accurate records of all email subscription requested, specifically including the email and associated headers sent by every subscriber, and shall immediately provide Premier Fiber with such records upon request. If a site has roaming users who wish to use a common mail server, the mail server must be configured to require user identification and authorization.
  
- Service must not be used to:
  - Send messages to any individual or entity who has indicated that they do not wish to receive a message from you.
  - Collect or redirect responses from unsolicited messages sent from accounts on other Internet hosts or messaging services which violate this policy, or the equivalent policy or any other policy of any other Internet service provider or website. Moreover, unsolicited messages sent from accounts on other Internet hosts or messaging services may not direct the recipient to any website or other resource that uses Premier Fiber's network.
  - Distributing Internet Viruses, Worms, Trojan Horses, flooding, mail bombing, or denial of service attacks or distributing information regarding the creation of such viruses, worms, etc. for reasons other than mitigation or prevention is prohibited.
  - Activities that disrupt the use of or interfere with the ability of others to effectively use the network or any connected network, system, service or equipment is prohibited.
  - Transmitting, distributing or storing information or material, that, as reasonably determined by Premier Fiber, is threatening, abusive, violates the privacy of others or which violates any applicable law or regulation, that is harmful to or interferes with Premier Fiber's provision of Service, the Premier Fiber network or any third party's network, equipment, applications, services or websites, that is fraudulent or contains false, deceptive or misleading statements, claims or representations (i.e., phishing), and deceptive marketing practices including, without limitation to, practices that violated United States Federal Trade Commission's guidelines for proper online marketing schemes is prohibited.



**No Resale/Sharing of Services:** Customers are prohibited from reselling the Service or otherwise making the Service available to third parties (for example, through Wi-Fi or other methods of networking), in whole or in part, directly or indirectly, unless expressly permitted by the Business Services Agreement or Master Services Agreement between the Customer and Premier Fiber;

Residential Customers agree that they will not make Services available to anyone other than their household and household guests. Business Customers will make services available only to authorized employees, unless done with Premier Fiber's prior written approval in accordance with an applicable Business Services Agreement or Master Services Agreement.

**Illegal Activity/Tortious Conduct:** Any use of the Services to violate any local, state or federal law or regulation, also violates this AUP. Prohibited activities include, but are not limited to:

- Services used to transmit, retransmit, distribute, post, or store any material that in the judgment of Premier Fiber is threatening, libelous, defamatory, or otherwise objectionable including but not limited to child pornography and advocating unlawful activity against any persons, animals, governments or businesses;
- Actions and/or Services prohibited by federal, state and local law;
- Posting, transmitting, downloading or viewing any material whatsoever pornographic in nature involving actual images of children or minors or digitally or otherwise artificially created or manipulated images of children or minors, or any material whatsoever that may be deemed obscene under applicable law;
- To violate Premier Fiber or any third party's copyright, trademark, proprietary or other intellectual property rights, including trade secret rights;
- Distribution, posting, copying or dissemination of copyrighted material including but not limited to movies and/or music;
- Participation in illegal gambling, lottery or other similar activities;
- Transmission of scams such as "Make Money Fast" schemes;
- Making fraudulent offers;
- Harassment of Customers, employees, or of others will not be tolerated;

## **SYSTEM & NETWORK SECURITY**

Violations of system or network security are prohibited, and may result in criminal and civil liability. Premier Fiber will investigate incidents involving such violations and may involve and will cooperate with law enforcement, if a criminal violation is suspected.

Examples of system or network violations include, without limitation the following:

- Unauthorized access to or use of computers, data, systems, accounts or networks, including any attempt to probe, scan, or test the vulnerability of a system or network or an attempt to penetrate security measures of another individual's system (known as 'hacking') is prohibited.
- 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 Customer, host or network including, without limitation, mail-bombing, flood, deliberate attempts to overload a system and broadcast attacks.
- Forging of any TCP-IP packet header or any part of the header information in an email or a newsgroup posting or otherwise engaging in any monitoring or interception of data not intended for the Customer without authorization is prohibited.
- Engaging in or permitting any network or hosting activity that results in the blacklisting or other blockage of Premier Fiber's IP space is prohibited.
- Also, attempting to circumvent Customer authentication or security of any hosts, network, or account ('cracking') without authorization is prohibited. Simulating communications ("phishing") from and/or to a website or other service of another entity in order to collect identity information, authentication credentials, or other information from the legitimate Customers of that entity's service is prohibited.
- Exporting encryption software over the Internet or otherwise in violation of ITAR, to points outside the United States is prohibited.
- Using malware, DNS cache poisoning or other means ("pharming") to redirect a Customer to a website or other service that simulates a service offered by a legitimate entity in order to collect identity information, authentication credentials, or other information from the legitimate Customers of that entity's service is prohibited.
- Activities that disrupt the use of or interfere with the ability of others to effectively use the Premier Fiber network, system, service, or equipment by utilizing programs, scripts, or commands to abuse a website (i.e., DDOS, SYN Floods or similar attacks)

**Web Hosting and Data Center Hosting Surveillance:** Premier Fiber performs routine surveillance of its networks in connection with its web hosting, data center hosting, and related services. Although Premier Fiber will not, as an ordinary practice, proactively monitor individual Customers' activities for violations of this AUP, there may be instances in which Premier Fiber, through its routine surveillance finds violations of this AUP and responds with appropriate action to immediately stop further violations at its sole discretion.

#### **CUSTOMER RESPONSIBILITY:**

Customers shall assume all risk associated with the activities referred to in the paragraphs above and Premier Fiber does not have any liability for any claims, losses, actions, damages,



suites or proceedings arising out of or otherwise relating to such activities.

**Risks of the Internet:** The internet, with its endless access to information, is a valuable tool but also a potential risk to safety and security. Customer should be aware of what they could become exposed to that includes, but not limited to:

- Downloading content (including receiving emails) from the Internet which may introduce viruses or other harmful features to the Customer's computer;
- Purchase goods or services using the Internet Transmitting confidential information over the Internet (such as credit card numbers or other business information), or some activities that Customers can perform when accessing the Internet may be harmful or cause loss to Customer, other people that may access Customer's service, or Customer's equipment without limitation;
- Accessing and viewing content on the Internet or otherwise available through the service that may be offensive to some individuals, or inappropriate for minors;
- Customers may minimize the risk of accessing illegal or offensive content as well as managing use of the Internet by using a filtering solution. Premier Fiber does not provide these filtering solutions as part of the Service and it is the Customer's responsibility to implement these measures.

**Password Security:** If applicable, Customer's password provides access to their individual Customer Portal. It is the responsibility of the Customer to keep their password secure. Customers are responsible for protecting their accounts and must take steps to ensure that others do not gain unauthorized access to the Customer's account or misuse Premier Fiber's Services. Attempting to obtain another Customer's account password is strictly prohibited.

**Call Recording:** Premier Fiber will provide a service whereby Customer will have the ability to record telephone calls between Customer or its representatives and third parties. Certain state and federal laws provide penalties in the event parties to a recorded telephone call have not consented to such recording.

In acknowledgment that Customer, and not Premier Fiber, will control how Customer's recording ability will be used, Customer shall indemnify and defend Premier Fiber, and its affiliated companies, and its and their respective officers, managers, directors, members, agents and employees, or any of them, from all causes of action, suits, losses, liabilities, claims, demands, judgments, penalties, fines, proceedings, direct costs, expenses (including reasonable attorneys' fees and costs), and damages, whether foreseen or unforeseen at the present time and whether based upon law or equity, contract or tort, or whether judicial or administrative in nature (collectively, "Losses"), arising in connection with claims asserted by third parties related to Customer's recording of telephone calls with third parties.

Customer assumes all responsibility for ensuring that recorded calls with third parties comply



with all federal laws and the laws in which Customer and third party are domiciled. Customer consents to Premier Fiber's recording of calls to the extent Premier Fiber can be considered as the party recording telephone calls for purposes of any state or federal law.

**CONTACT INFORMATION:**

**Contact for Reporting Abuse:** Any party seeking to report a violation of this AUP may contact Premier Fiber via email at [support@premierfiber.com](mailto:support@premierfiber.com).

**Contact for Copyright Infringement:** Premier Fiber complies with the Online Copyright Infringement Liability Limitation Act of 1998. 17 USC 512 ("Act"). As required by the Act, Premier Fiber has a policy that reserves its right to terminate services to subscribers who repeatedly infringe copyrights. In the event that Premier Fiber receives a determination that any subscriber or account holder has infringed another's copyright through the use of its system or network, Premier Fiber reserves the right to terminate service to that subscriber immediately. Premier Fiber accommodates and does not interfere with standard technical measures to identify and protect copyrighted works, subject to the limitations of the Act.

Notices and counter-notices related to claimed copyright infringements should be directed to the following designated agent: [support@premierfiber.com](mailto:support@premierfiber.com).