SINLAR BROADBAND Acceptable Use Policy (AUP)

Background

THIS ACCEPTABLE USE POLICY (AUP) IS A MATERIAL PART OF ANY CUSTOMER AGREEMENT WITH SINLAR BROADBAND, FOR THE PROVISION OF SERVICE(S). BY YOUR USE AND ACCEPTANCE OF SINLAR BROADBAND' SERVICE(S), YOU ARE ACKNOWLEDGING THAT YOU ARE OF LEGAL AGE AND HAVE READ, UNDERSTAND AND AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THE AGREEMENT PRESENTED. IF YOU DO NOT ACCEPT THIS AUP, DO NOT USE THE SERVICE(S) PROVIDED BY SINLAR BROADBAND.

SINLAR BROADBAND RESERVES THE RIGHT TO CHANGE THIS AUP AT ANY TIME AND ANY MODIFICATION(S) SHALL BE EFFECTIVE WHEN POSTED. YOUR CONTINUED USE OF SERVICES AFTER CHANGES ARE POSTED CONSTITUTES YOUR ACCEPTANCE OF ANY SUCH MODIFICATION(S).

VIOLATION OF ANY PROVISION OF THIS AUP MAY RESULT IN THE IMMEDIATE TERMINATION OR SUSPENSION OF THE SERVICES YOU RECEIVE FROM SINLAR BROADBAND. YOU SHALL REMAIN SOLELY LIABLE AND RESPONSIBLE FOR YOUR USE OF THE SERVICES AND ANY AND ALL CONTENT THAT YOU DISPLAY, UPLOAD, DOWNLOAD OR TRANSMIT THROUGH THE USE OF THE SERVICES. "CONTENT" INCLUDES, WITHOUT LIMITATION, YOUR E-MAIL, WEB PAGES, PERSONAL HOME PAGES, AND DOMAIN NAMES. NO CREDITS WILL BE ISSUED FOR AN INTERRUPTION IN SERVICE RESULTING FROM AUP VIOLATIONS.

1. USE

The Service is designed solely for use in Customer's Residential or business location, Determined on activation date and/or location of installed equipment. Customer is responsible for any misuse of the Service that occurs through Customer's account, whether by an employee of Customer's business or an authorized or unauthorized third-party. Customer is responsible for any and all e-mail addresses associated with the Customer's account. Customer must take steps to ensure that others do not gain unauthorized access to the Service. Customer is solely responsible for the security of (i) any device Customer chooses to connect to the Service, including any data stored or shared on that device and (ii) any access point to the Service. If the Customer sells or resells advertising or web space to a third party, then the Customer will be responsible for the content of such advertising or on such web space and the actions of such third party. Customer will not resell or redistribute, or enable others to resell or redistribute, access to the Service in any manner, including, but not limited to, wireless technology, except as expressly provided in any contract for service. Sinlar Broadband reserves the right to disconnect or

reclassify the Service to a higher grade or to immediately suspend or terminate the Service for failure to comply with any portion of this provision or this Policy, without prior notice.

2. PROHIBITED ACTIVITIES USING THE SYSTEM, NETWORK, AND SERVICE

Any activity or use of the Service which violates system or network security or integrity are prohibited and may result in criminal and civil liability. Such violations include, without limitation, the following:

A) 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, relay communication through a resource, or to breach security or authentication measures without express authorization of the owner of the system or network.

B) Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner or network.

C) Interference with service to any user, host, or network, including but not limited to: mail bombing, flooding, or denial of service attacks.

D) Forging the header of any transmitted information packet, email, or Usenet posting.

E) Modifying or tampering with any hardware, software, or configuration provided by Sinlar Broadband including but not limited to: routers, switches, access points, wireless gateways, security devices and cable modem configuration files.
E) Reselling or otherwise redistributing the Service, disrupting any aspect of the Service through any means.
F) Excessive use of bandwidth that in Sinlar Broadband's sole opinion, places an unusually large burden on the network or is deemed by Sinlar Broadband to be above normal usage.
G) Sinlar Broadband has the right to impose limits on excessive bandwidth consumption via any means available to Sinlar Broadband.

H) Assuming or assigning a Sinlar Broadband IP address that was not allocated to the user by Sinlar Broadband or its network - all Sinlar Broadband Internet users must use DHCP assigned by the Service to acquire an IP address or utilize a Static IP address provided by Sinlar Broadband.

I) Running any type of server on Sinlar Broadband's system that is intentionally used to disrupt other users of the Service or users of the Internet in general.

3. NO ILLEGAL OR FRAUDULENT USE

The Service may be used only for lawful purposes. Customer will not use or allow others to use the service in any manner that is in violation of any applicable federal, state, local or international laws or regulations or to promote, engage in, or enable illegal activity or conduct that violates or infringes upon the rights of any person. Transmission or distribution of any

material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret, or other intellectual property right used without proper authorization, and material that is obscene illegal, defamatory, constitutes an illegal threat, or violates export control laws. Furthermore, use of the Service to impersonate a person or entity is not permitted.

4. NO COPYRIGHT OR TRADEMARK INFRINGEMENT

Use of the service is also subject to Sinlar Broadband's Copyright Infringement Policy. Sinlar Broadband reserves the right to suspend or terminate accounts which are in violation of Sinlar Broadband's Copyright Infringement Policy.

5. NO SPAM

Users may not send any unsolicited bulk email or electronic communication including, but not limited to, instant messenger programs, IRC, Usenet, etc. that promotes or advertises a cause, opinion, money making opportunity, or the like that the recipient did not specifically request from the sender ("Spam").

All commercial email messaging must comply with the Federal, State, and Local law, such as the CAN-SPAM Act (See: http://www.business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business and http://uscode.house.gov/download/pls/15C103.txt) These communications do not necessarily have to pass through the Service's email infrastructure - it only needs to originate from a Service User.

Sinlar Broadband maintains a zero-tolerance policy on Spam for all of its Internet products and may take immediate action against users violating this AUP. Sinlar Broadband reserves the right to impose certain limitations on use of the Service's email.

The Services may not be used to collect responses from unsolicited communication regardless of the communication's origination. Moreover, unsolicited communication may not direct the recipient to any web site or other resource that uses the Service and the user may not reference the Service in the header or by listing an IP address that belongs to the Service in any unsolicited communication even if that communication is not sent through the Service or its infrastructure.

Users may not send any type of communication to any individual who has indicated that he/she does not wish to receive messages from them. Continuing to send email messages to anyone that has expressly requested not to receive email from a User is considered to be harassment. . Customer is responsible for maintaining confirmed opt-in records and must provide them to Sinlar Broadband upon request. The term "opt-in" means that recipient has signed up for mailings voluntarily.

6. NO SYSTEM DISRUPTION

Customer will not use, or allow others to use, the Service to disrupt degrade, and/or otherwise adversely affect Sinlar Broadband's network or computer equipment owned by Sinlar Broadband or other Sinlar Broadband customers.

7. SECURITY/ABUSABLE RESOURCES

System and Network Security

Violations of system or network security may result in criminal and civil liability. Sinlar Broadband may 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 security violations include, without limitation, the following:

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.

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, mail bombing, flooding, 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.

Violators of the policy are responsible, without limitations, for the cost of labor to clean up and correct any damage done to the operation of the network and business operations supported by the network, and to respond to complaints incurred by Sinlar Broadband. Such labor is categorized as emergency security breach recovery and is currently charged at $250 USD per hour required. Enquiries regarding security matters may be directed to support@sinlarbroadband.com

User is solely responsible for the security of any device connected to the Service, including any data stored on that device. Users shall take all necessary steps to avoid actions that result in the abuse of a resource on their network. Examples of abusable resources include but are not limited to: open news servers, open SMTP servers, insecure routers, wireless access and insecure proxy servers. Upon notification from Sinlar Broadband, Users are required to address the problem in a timely fashion. Failure to address an issue after notification will be considered a violation of this AUP.

8. NO "HACKING"

Customer will not use, nor allow others to use, the Service to access the accounts of others or to attempt to penetrate security measures of the Service or other computer systems ("hacking") or to cause a disruption of the Service to other on-line users. Customer will not use, nor allow others to use, tools designed for compromising network security, such as password-guessing programs, cracking tools, packet sniffers or network probing tools.

Child Pornography on the Internet

Sinlar Broadband will cooperate fully with any criminal investigation into a Customer's violation of the Child Protection Act of 1984 concerning child pornography. Customers are ultimately responsible for their actions over the Sinlar Broadband network, and will be liable for illegal material accessed or posted. Violations of the Child Protection Act may be reported to the U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) at 1-866-

DHS-2-ICE. Suspected child sexual exploitation or missing children may be reported to the National Center for Missing & Exploited Children via its toll-free 24-hour hotline, 1-800-THE-LOST.

9. NETWORK MANAGEMENT

Sinlar Broadband reserves the right to use a changing variety of reasonable network management techniques including but not limited to (i) allocation a fixed maximum amount of bandwidth to non-customers seeking to upload peer-to-peer files from customers; (ii) utilizing STM technology to prioritize traffic during times of peak congestion; and (iii) implementing filtering and spam detection techniques to manage reliable email sources and mitigate spam. In limited instances, these techniques may affect the throughput rate at which customers may send and receive data, non-customers' ability to establish session connections within the network (such as peer-to-peer sessions), or result in the delay of certain traffic during times of peak congestion.

10. Viruses

Users must take appropriate action to prevent their systems from becoming infected with and/or distributing computer viruses such as but not limited to worms, "Trojan horses", denial of service attacks bots. Sinlar Broadband will take appropriate (as decided by Sinlar Broadband's sole discretion) action against Users infected with computer viruses or worms to prevent further spread.

11. ENFORCEMENT

Sinlar Broadband reserves the right to investigate violations of this AUP, including the gathering of information from the Customer or other Users involved and the complaining party, if any, and the examination of material on Sinlar Broadband's servers and network. Sinlar Broadband prefers to advise Users of AUP violations and any necessary corrective action but, if Sinlar Broadband, in its sole discretion, determines that a User has violated the AUP, Sinlar Broadband will take any responsive action that is deemed appropriate without prior notification. Such action includes but is not limited to: temporary suspension of service, reduction of service resources, and termination of service. Sinlar Broadband is not liable for any such responsive action and these actions are not exclusive. Sinlar Broadband may take any other legal or technical action it deems appropriate.

Last updated November 23rd 2016