Rebeltec Communications LLC

ACCEPTABLE USAGE POLICY

This Acceptable Use Policy (AUP) sets forth guidelines for customers, subscribers, and clients of Rebeltec Communications, LLC (Rebeltec) who connect to and use any of the computer networks belonging to Rebeltec and in which Rebeltec has administrative authority. This includes radio networks, wireless networks, Ethernet networks, fiber networks, and any other form of subscription and/or connectivity used. The latest version of this AUP is available at the URL http://www.rebeltec.net/UsagePolicy.html. Changes or modifications to this AUP will be effective immediately upon posting to that URL.

INTRODUCTION

Among other services, Rebeltec provides network connectivity for Internet access. Rebeltec makes little attempt to filter or control the content of data and information entering its networks upon request of network users (by actions such as browsing the World Wide Web, downloading files or documents, or participating in online conversations). Illegal activity is explicitly prohibited, and Rebeltec may take efforts to protect its customers and its own computing/network equipment from known spammers (via the Real-Time Black List) and potential vulnerabilities. Rebeltec does not make any warranty or guarantee of protection from network-based, application-based, or any other kind of attacks or attempts to control the computing equipment of its customers. Rebeltec strongly encourages users to become aware of potential vulnerabilities and forms of computer and network attacks, and to take measures to eliminate and protect against them (use firewalls, virus scanning software, install OS updates, etc.). Rebeltec exerts some control over the content of data and information originating from and the use of its networks and services made available to customers. It is not Rebeltec's intent to deny or prohibit legitimate use of the Internet. There are both legal and practical obligations of an Internet Service Provider to contain the bounds of what use of its services is allowed and (especially) disallowed. As outlined herein, the Rebeltec AUP goes beyond the requirements to simply comply legally with the current laws by imposing certain limits and restrictions on behavior and use of Internet services by its network users, though the behavior may not explicitly be illegal. Our aim is to aid in eliminating network/Internet abuse and misuse, as well as to protect ourselves and our users from adverse consequences that result when not doing so.

Sending Unsolicited Commercial Email (UCE) can result in being put on a "blacklist" such that all I users could be affected by the inability to send mail, or make any network connections at all sites that choose to honor the blacklist. Therefore sending UCE (also known as "Spam") is against this AUP, even though it may not be explicitly illegal.

The following are examples of conduct that may lead to termination of your Service:

- Access, without permission or right, the accounts or computer systems of others to spoof the URL, DNS, or IP addresses of any other entity or to penetrate the security measures of the network or any other computer system or attempt any of the foregoing activities;
- Transmit uninvited communications, data, or information, or engage into similar activities, including without limitation "spamming," "flaming," or denial of service attacks;
- Intercept, interfere with or redirect email or any other transmissions sent by other users;
- Upload viruses, worms, Trojans, or any other harmful code on the internet;
- Engage in conduct that is defamatory, fraudulent, obscene, or deceptive;
- Violate any third party's copyright, trademark, proprietary, or other intellectual property rights;
- Generate excessive amounts of email or other internet traffic; or
- Use internet service in any way, for the transmission or dissemination of images containing child pornography or in a manner that is obscene, sexually explicit, cruel, or racist in nature or which espouses, promotes, or incites bigotry, hatred, or racism.

ILLEGAL ACTIVITY

Rebeltec explicitly disallows any activity or use of networks and services in which are in violation of any local, regional, state or federal law or ordinance. Customers may not post, retrieve, transmit, or store material on or through Rebeltec equipment or networks that is in violation of any applicable law or regulation, including material that is threatening, defamatory, obscene, indecent, constitutes an illegal threat, or could otherwise adversely affect any individual, group or entity, as well as material that is protected by copyright, trademark, patent, trade secret or other intellectual property law.

Installation, storage, or distribution of licensed software without having appropriate license (a.k.a. "pirate" or "warez" software) is prohibited. Should evidence of such activity be produced to or encountered by Rebeltec, investigation may be made and/or corrective action taken in the matter possibly including, but not limited to account suspension and/or termination and involvement with appropriate law enforcement officials.

COPYRIGHT INFRINGEMENT/REPEAT INFRINGER

Customers may not post, retrieve, transmit, or store material on or through Rebeltec equipment or networks that constitutes an infringement of any third party intellectual property rights, per copyright law. It is the policy of Rebeltec to suspend or terminate, under certain conditions, the Services provided to Subscribers who is deemed to infringe on third party intellectual property rights, especially repeat infringers. Rebeltec reserves the right to suspend/terminate, or take any other interim action regarding internet service if Rebeltec, in its sole discretion, believes that circumstances relating to an infringement of third party intellectual property rights demand such action. If subscriber believes that copyrighted material has been used in violation of this policy or has been made available on the Service in a manner not authorized by the copyright owner, agent or authorized user, please contact Rebeltec at abuse@rebeltec.net.

EMAIL / USENET NEWS

Sending unsolicited commercial email (UCE) advertisements or informational announcements, chain letters, and "junk mail," as well as posting similar news messages to unrelated news groups or posting a message to multiple newsgroups, collectively known as "spam," is prohibited. Forging any Email or News header or providing false information during a SMTP conversation is prohibited. Additionally, using non-Rebeltec servers or services to relay mail or news either without permission or in order to send spam is prohibited. Rebeltec does not monitor the content of outgoing Email or News postings, but does respond to reports of abuse of either, typically with account termination. Rebeltec does cooperate with law enforcement personnel in determining the origin of threatening messages and regarding similar issues.

SYSTEM/NETWORK SECURITY

Attempting to defeat system or network security mechanisms, probe or scan systems and/or networks, forge network or application information, or cause a denial of service (DoS) to any system or network is explicitly forbidden, whether the system(s) and/or network(s) involved belong to Rebeltec or otherwise, without express permission of the owner of the system/network. This includes, among similar activities, all of the following:

• Intercepting or diverting information, whether in transit or stored, for which you are not the intended recipient or would otherwise be allowed access to.
• Forging any part of an Email or News header, or information in headers of TCP/IP network packets.
• Using accounts for which you are not authorized to use, attempting to retrieve or determine account names and passwords, or otherwise attempting to bypass or manipulate an authentication system.
• Attempting to probe or scan systems or networks to determine potential vulnerabilities, services available, operating systems in use, or in order to map networks.
• Mail bombing and network flooding (ping floods, broadcast attacks, and the like).
• Attempting to cause any machine or application to crash or to consume resources such that services become unavailable or interrupted.

REPORTING SYSTEM / NETWORK / SERVICE ABUSE

Complaints, reports or concerns of illegal activity, or activity in violation of the terms of this AUP and originating within or upstream of Rebeltec's networks, including SPAM (UCE) should be directed to abuse@rebeltec.net. Complaints or reports of such activity originating outside Rebeltec (and upstream) networks should be directed to the authorities of the respective source. There is detailed information to help in determining such contact information available at http://spam.abuse.net/howtocomplain.html.