Acceptable Use Policy

As a provider of Internet access, Internet email, web site hosting, Google Apps, and other Internet-related services, Cimarron Telephone and CimTel.net ("the Provider") offers its subscribers (and their customers and users), the means to access and disseminate a wealth of information. The Provider respects that the Internet provides a forum for free and open discussion and dissemination of information. However, there are competing interests at issue. The Provider reserves the right to take certain preventative or corrective actions as deemed necessary. In order to protect these competing interests, the Provider has developed an Acceptable Use Policy ("AUP"), which supplements and explains certain terms of each customer's respective service agreement and is intended as a guide to the customer's rights and obligations when utilizing the Provider's services. This AUP will be revised from time to time. A customer's use of the Provider's services after changes to the AUP are posted on the Provider's web site, www.cimtel.net, will constitute the customer's acceptance of any changes to the AUP.

Email: Email accounts not accessed in 90 days will be archived for deletion. Once an email account has not been accessed in 120 days, that account will be purged from the system.

Email and Apps:
Provider's email platform, and certain other applications may be provided by third parties.. A customer's use of third-party email or other applications may be governed by both Provider's AUP and the third-party application provider's AUP or terms of service, and subscribers are responsible for compliance with all AUPs or terms of service applicable to the service and applications being used.

Prohibited Activities: When subscribers disseminate information through the Internet, they also must keep in mind that the Provider does not review, edit, censor, or take responsibility for any information its subscribers may create. When users place information on the Internet, they have the same liability as other authors for copyright infringement, defamation, and other harmful speech. Also, information created and carried over the Provider's network may reach a large number of people, including both subscribers and nonsubscribers of the Provider, possibly affecting other subscribers and may harm the Provider's goodwill, business reputation, and operations. For these and other reasons, the Provider has developed an AUP to define prohibited activities:

Spamming: Spamming is sending unsolicited bulk and/or commercial messages over the Internet. It is harmful not only because of its negative impact on consumer attitudes toward the Provider, but also because it can overload the Provider's network and disrupt service to the Provider's subscribers. Such behavior could result in the Provider's mailservers being blacklisted by various anti-spamming organizations subscribed to by other Internet service providers, thus denying the Provider's subscribers access to other parts of the Internet. Also, creating, operating or maintaining an open SMTP relay is prohibited. The only acceptable method for creating and maintaining a mailing list for unsolicited commercial e-mail (UCE) or unsolicited bulk e-mail (UBE) is to have subscribers opt in to the list using secure sockets layer (SSL) authentication, or other means where the user can be positively identified by means of a digital "signature" and the user's choice to receive the bulk or commercial mailings is clear. Opt-out lists, and double-negative lists are specifically prohibited. The existence of a "business relationship" between the entity sending and the individual receiving UCE or UBE is not an acceptable justification for the dissemination of UCE or UBE, unless the customer has specifically "opted-in" via verifiable SSL webpage or specific, verifiable request via e-mail. When a complaint is received, the Provider has the discretion to determine from all of the evidence whether the email recipients were from an acceptable "opt-in" email list. Maintainers of such bulk mailing lists are required to keep verifiable evidence, to include logs for SSL-verified opt-in webpages, or complete headers and text for e-mail requests for a period of 120 days after the addition of each e-mail address to the list. The maintainer of such lists must present this evidence to the Provider upon request. Any domains hosted by the Provider must have working, active mailboxes maintained for "abuse" and "postmaster" aliases. Failure of a responsible party in the company hosted to answer e-mail received by either the postmaster or abuse aliases shall be grounds for termination of the account concerned. The Provider proactively opposes spamming in all forms, and it is the Provider's policy to immediately interrupt traffic in progress, and terminate subscriber service that may potentially pose harm to the Provider's business reputation and operations. The Provider reserves the right to terminate, with or without notice, the account of any webhosted service whose website is advertised by or referred to in UCE or UBE. This activity, known as "spamvertising" or the site, known as a "spamvertised website" is specifically prohibited under the terms of this policy.

Intellectual Property Violations: Intellectual property violations include engaging in any activity that infringes or misappropriates the intellectual property rights of others, including copyrights, trademarks, service marks, trade secrets, software piracy, and patents held by individuals, corporations, or other entities. Also, engaging in activity that violates privacy, publicity, or other personal rights of others.
We comply with the Online Copyright Infringement Liability Limitation Act of 1998 ("Act"). As required by the Act, we have adapted a policy to suspend or terminate services to account holders or subscribers who repeatedly infringe copyrights. Upon receipt of a notification that any subscriber or account holder has infringed another's copyright through the use of our system or network, we reserve the right to terminate service to that subscriber or account holder after receiving notice of any further copyright infringement by that subscriber or account holder. We accommodate and do not interfere with standard technical measures to identify and protect copyrighted works, subject to the limitations of the Act.

In accordance with the Online Copyright Infringement Liability Limitation Act, 17 USC § 512(c)(2), we have filed with the United States Copyright Office the necessary designated agent information to facilitate notice of alleged online copyright infringement on our network. Our designated agent for notification of alleged copyright infringement and counter notification is:

Kristy Young
101 Cimarron Street
Mannford, OK 74044
P: 918.865.3311
F: 918.865.3187
copyright@mbo.one

Obscene Speech or Materials: Obscene speech or materials can include using the Provider's network to advertise, transmit, store, post, display, or otherwise make available child pornography or obscene speech or material. The Provider is required by law to notify law enforcement agencies when it becomes aware of the presence of child pornography on or being transmitted through the Provider's network. Using the Provider's network as a means to transmit or post defamatory, harassing, abusive, or threatening language is also prohibited and grounds for immediate termination of the account concerned, as well as the release of all logs containing such language to the proper investigative government authorities.

Forging of Headers: Forging or misrepresenting message headers, whether in whole or in part, to mask the originator of the message.

Illegal or Unauthorized Access to Other Computers or Networks: Accessing illegally or without proper authorization, any computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system (often known as "hacking"). This includes any activity that might be used as a precursor to an attempted system penetration (i.e. port scan, stealth scan, or other information gathering activity). Knowingly engaging in any activities that will cause a denial-of-service (e.g., synchronized number sequence attacks) to any of the Provider customers or end-users whether on the Provider's network or on another provider's network. Accessing services not included or not paying for. This includes but is not limited to circumventing security, interfering with a service, overloading a service, disabling a host, encumbering disk space processors or other system resources.

Distribution of Internet Viruses, Worms, Trojan Horses, or Other Destructive Activities: Distributing information regarding the creation of, and sending Internet viruses, worms, Trojan horses, pinging, flooding, mailbombing, or denial of service attacks. Also, 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. The Provider may suspend activity of any account whose computer(s) have become infected by a worm or trojan horse type virus, causing the computer to generate unsolicited e-mails, or where the danger of infecting other users on the Provider's network or any other network is present.

Facilitating a Violation of this AUP: Advertising, transmitting, or otherwise making available any software, program, product, or service that is designed to violate this AUP, which includes the facilitation of the means to spam, initiation of pinging, flooding, mailbombing, denial of service attacks, and piracy of software.

Export Control Violations: Exporting software over the Internet or otherwise to points outside the United States in violation of export control laws or regulations.

Usenet Groups: The Provider reserves the right not to accept postings or deliver messages from newsgroups where we have actual knowledge that the content of the newsgroup violates the Provider's AUP.

Other Illegal Activities: Engaging in activities that are determined to be illegal, including advertising, transmitting, or otherwise making available ponzi schemes, pyramid schemes, fraudulently charging credit cards, and pirating software.
Internet connections and all other services provided to the subscriber may only be used for lawful purposes. Transmission or storage of any information, data or material in violation of any U.S. Federal or state regulation or law is prohibited.

Other Activities: Engaging in activities, whether lawful or unlawful, that the Provider determines to be harmful to its subscribers, operations, reputation, goodwill, or customer relations.

IRC: The Provider does not allow, maintain, provide, nor support Internet Relay Chat services.

Account Security: You are also solely and fully responsible and liable for all activities that occur under your account. You have sole responsibility for ensuring that anyone who uses the Services through your account understands and complies with this AUP. You further acknowledge and agree that you are solely responsible and liable for any violations of the terms of this AUP, whether by you or by any other user of the Services through your account.

Grant of License: The Provider is granted world-wide, royalty free and non-exclusive license(s) to any content you submit or make available for inclusion on publicly accessible areas of Provider's website ("the Site"). With respect to content, photos, graphics, audio or video you submit or make available for inclusion on publicly accessible areas you grant the license to use, distribute, reproduce, modify, adapt, publicly perform and publicly display such content, photos, graphics, audio or video only for as long as you elect to continue to include such content, photos, graphics, audio or video and will terminate at the time you disconnect service.

Policy Enforcement: The Provider will not, as an ordinary practice, monitor the communications of its subscribers to ensure that they comply with this AUP or applicable law. When the Provider becomes aware of unauthorized activities, however, it may take any action to stop the unauthorized activity, including but not limited to, removing information, shutting down a web site, implementing screening software designed to block offending transmissions, denying access to the Internet, or take any other action it deems appropriate. If such violation is a criminal offense, the Provider will notify the appropriate law enforcement department of such violation.

Third Party: It is a violation of this AUP for a subscriber to resell or redistribute Provider's services, including via wi-fi hot spots, without Provider's prior written consent. Any subscriber who, with Provider's written consent, resells or redistributes Provider's services is responsible for violations of this AUP by anyone receiving the services from the subscriber. The use of private IP addressing behind a public IP by a customer is done so at the customer's risk. Any malicious activity originating from a public IP may result in the Provider shutting down that IP, regardless of the number of users behind that address. This can include any activity that impacts the Provider's network or violates the Provider's AUP and can result in an interruption of service. It is the responsibility of the customer to trace private IP traffic for, but not limited to, the enforcement of the provider's Internet AUP and tracing illegal activity.

Privacy: The Provider also is concerned with the privacy of on-line communications and web sites. In general, the Internet is neither more nor less secure than other means of communication, including mail, facsimile, and voice telephone service, all of which can be intercepted and otherwise compromised. As a matter of prudence, however, the Provider urges its subscribers to assume that all of their on-line communications are insecure. The Provider cannot take any responsibility for the security, accuracy, or delivery of information transmitted over the Provider's facilities.

Legal: The Provider cannot monitor, verify, warrant, or vouch for the accuracy and quality of the information that subscribers may acquire. For this reason, the subscriber must exercise his or her best judgment in relying on information obtained from the Internet, and also should be aware that some material posted to the Internet is sexually explicit or otherwise offensive. Because the Provider cannot monitor or censor the Internet, and will not attempt to do so, the Provider cannot and does not accept any responsibility for damages or injury that result from information or communications on the Internet.

We hope this AUP is helpful in clarifying the obligations of Internet users, including the Provider and its subscribers, as responsible members of the Internet. Any complaints about a subscriber's violation of this AUP should be sent to abuse@mbo.one.