

Acceptable Use and Network Management Policy of Home TeleNetworks, Inc.

By using Service(s) provided by Home TeleNetworks, Inc., and its affiliates or subsidiaries (all hereafter referred to as "HomeTel"), you ("Customer") agree to comply with this Acceptable Use and Network Management Policy ("AUP").

Introduction:

The purpose of this AUP is to inform our customers of our expectations regarding their use of the Internet through the HomeTel Network. It is binding on all users of the HomeTel Network. This policy should be read in conjunction with the HomeTel Internet Access Agreement, the HomeTel Abuse Policy, the HomeTel Privacy Policy, and all other policies published by HomeTel. This AUP may be revised from time to time, and your use of HomeTel's Service(s) after changes are posted on HomeTel's web site at <http://www.hometel.com/internet/policies/> shall constitute your acceptance of any changes or additional terms. The HomeTel AUP is designed to help protect HomeTel's assets, the assets of its Customers, and the Internet community, from irresponsible or illegal activities of HomeTel Customers or their Users. These activities may disrupt or degrade HomeTel Services, pose a threat to HomeTel's assets, expose HomeTel (or other providers of Internet Services) to claims of civil or criminal liability or other legal sanctions. Moreover, because of various conventions used in the industry (including blocking, filtering and blacklisting) these activities may impair HomeTel's ability to interconnect with other providers of Internet Service. These activities may relate to the content stored or transmitted by Customers or their Users or to the nature of the transmissions themselves such as sending large numbers of unsolicited messages (Spam). Customers are responsible for avoiding the prohibited activities and strictly following the AUP terms set forth herein.

HomeTel commits to the open and non-discriminatory use of the Internet by its customers and commits to use reasonable network management practices to ensure an open Internet. HomeTel will manage its network and provide access in accordance with the Federal Communications Commission's (FCC's) Open Internet Rules (adopted December 21, 2010 in 25 FCC Rcd 17905) and in compliance with any future rules adopted by the FCC.

Transparency:

HomeTel shall make available public information on its website (<http://www.hometel.com/internet/policies/>) regarding its network management practices, performance and commercial terms of its service sufficient for consumers to make an informed choice regarding their use of such services. HomeTel will not unjustly or unreasonably prevent or interfere with competition among Content, Applications, Service, or Device Providers.

AUP Coverage:

This HomeTel AUP applies to the Services that provide (or include) access to the Internet, Services provided over the Internet, and Hosting services (collectively "IP Services"). Customer is responsible for the actions of all others who may be using the IP Service(s) under Customer's account. It is Customer's obligation to take whatever measures are necessary to protect access to a Customer account. This may include, but is not limited to, the protection of passwords. If a Customer or its User(s) violate the AUP, HomeTel may, depending on the nature and severity of the violation, suspend or terminate service, as specified below. Customer may have access through the HomeTel Network(s) and Service(s) to search engines, subscription web services, chat areas, bulletin boards, web pages, USENET, or other services that promulgate rules, guidelines or agreements to govern their use. Failure to adhere to any such rules, guidelines, or agreements shall be a violation of this AUP.

AUP Enforcement and Notice:

Customer's failure to observe the guidelines set forth in this AUP may result in HomeTel taking actions, anywhere from a warning to a suspension of privileges or termination of your Service(s). HomeTel reserves the right, but does not assume the obligation, to strictly enforce the AUP. When feasible, HomeTel may provide Customer with notice of an AUP violation via e-mail or otherwise, and demand that such violation be immediately corrected. However, HomeTel reserves the right to act immediately and without notice to suspend or terminate IP Service(s) in response to a court order or other legal requirement that certain conduct should be stopped or when HomeTel determines, in its sole discretion, that the conduct may: (1) expose HomeTel to sanctions, prosecution, civil action or any other liability, (2) cause harm to or interfere with the integrity or normal operations of HomeTel's network(s) or facilities, (3) interfere with another person's use of HomeTel's IP Service(s) or the Internet, or (4) otherwise present a risk of harm to HomeTel or HomeTel Customers, or other parties HomeTel interconnects with. HomeTel's decisions with respect to interpretation of the AUP and appropriate remedial actions are final and determined by HomeTel in its sole discretion. HomeTel may refer potential violations of law(s) to the proper authorities, may cooperate in

the investigation of any suspected criminal or civil wrongdoing, and will cooperate with authorities when required to do so by law, subpoena, or when the public safety is at stake. HomeTel assumes no obligation to inform Customers that their information has been disclosed, and, in some cases, may be prohibited by law from providing such notice. HomeTel does not, as an ordinary practice, proactively monitor the activities of those who use its IP Service(s) or exercise any editorial control over any material transmitted, hosted or posted using IP Services to ensure that its Customers comply with the AUP and/or the law, although it reserves the right to do so. If HomeTel is alerted to violations, or potential violations, of this AUP, HomeTel will take whatever measures it deems necessary and appropriate to stop or prevent such violations, including the actions described in this AUP. For example, HomeTel may in its sole discretion refuse to transmit, screen, or edit content prior to delivery of the IP Service(s), block access to certain categories of numbers or certain sites as HomeTel determines needed to enforce these policies. If Customer's Service is suspended or terminated for any AUP violation, Customer must get written approval from HomeTel's Policy Management Department (to reactivate service, or order new service. HomeTel may, in its discretion, decline to reinstate Customer's Service. If HomeTel's Policy Management Department approves Customer for reinstatement or new service, set-up fees, reactivation fees or deposits may apply. If HomeTel discovers that Customer has renewed Service, or ordered new Service, following termination for an AUP violation without the prior written consent of the HomeTel Policy Management Department, HomeTel may terminate your Service without further notice. In such case, Customer is responsible for any applicable early termination charges. HomeTel will not issue any refunds, credits or other forms of compensation for the period when IP Service(s) have been suspended as a result of violation(s) or alleged violation(s) of this AUP. HomeTel shall not be liable for any damages of any nature suffered by any Customer, User, or third party resulting in whole or in part from HomeTel's exercise of its rights under this AUP.

Network Security:

HomeTel uses generally accepted technical measures to provide acceptable service levels to all customers, such as application-neutral bandwidth allocation, as well as measures to address service attacks, illegal content and other harmful activities to protect network integrity and reliability.

Prohibited Actions:

Customer may not use the Service in a manner that violates any applicable local, state, federal or international law, order or regulation. Additionally, the customer may not use the HomeTel IP Services to:

- Conduct, participate in, or otherwise facilitate pyramid or other illegal soliciting schemes.
- Take part in any fraudulent activities, including impersonating any person or entity or forging anyone else's digital or manual signature.
- Invade another person's privacy, stalk, harass, or otherwise violate the rights of others.
- Post, transmit, or disseminate content that is illegal, threatening, abusive, libelous, slanderous, defamatory, promotes violence, or is otherwise offensive or objectionable.
- Restrict, inhibit, or otherwise interfere with the ability of any other person to use or enjoy the equipment or the Service, including, without limitation, by posting or transmitting any information or software which contains a virus, lock, key, bomb, worm, Trojan horse, Cancelbot, or other harmful feature.
- Collect or store personal data about other users.
- Use an IP address not assigned to the Customer.
- Violate any other HomeTel policy or guideline.
- Resell or redistribute the Service to any third party via any means including but not limited to wireless technology.

Unlawful Activities:

HomeTel IP Services shall not be used in connection with any criminal, civil or administrative violation of any applicable local, state, and provincial, federal, national or international law, treaty, court order, ordinance, regulation or administrative rule. By using the HomeTel IP Service(s), Customer represents and warrants to HomeTel that Customer (and its Users) are not resident(s) of any country, or affiliated with, any other organization prohibited to do business within the United States as defined by the Office of Foreign Assets Control within the United States Department of the Treasury.

Intellectual Property:

You are prohibited from infringing, publishing, submitting, copying, uploading, downloading, posting, transmitting, reproducing, or distributing software, video or audio content, or any other material that is protected by copyright, trademark, patent, trade secret, any other type of intellectual property rights, trademark laws (by rights of privacy or publicity) or other proprietary right of any party unless you own or control the rights thereto or have received all necessary consent to do the same. This prohibition includes the use of any material or information including images or photographs that are made available through any HomeTel site or Service(s). For more information about HomeTel's copyright protection practices under the Digital

Millennium Copyright Act (DMCA) of 1998 or for information on how to contact HomeTel's DMCA agent, please contact HomeTel's Policy Management Department whose contact information is listed below.

Offensive or Threatening Material or Content:

HomeTel IP Services shall not be used to host, post, transmit, or re-transmit any content or material that is threatening, harassing, obscene, indecent, hateful, malicious, racist, fraudulent, deceptive, invasive of privacy or publicity rights, abusive, inflammatory, or otherwise harmful or offensive to third parties, treasonous, excessively violent or promotes the use of violence, or provides instruction, information or assistance in causing or carrying out violence against any government, organization, group or individual, or provides guidance, information or assistance with respect to causing damage or security breaches to HomeTel's Network or to the network of any other IP Service provider. Customer shall not create or attempt to utilize a domain name that is fraudulent, indecent, offensive, deceptive, threatening, abusive or harassing.

Interaction with Minors:

HomeTel has a zero tolerance policy regarding use of its Service to engage in inappropriate conduct with a minor (anyone under 18 years of age). You shall not knowingly collect or solicit personal information from a minor without the express consent of the parent or guardian of the minor, nor shall you use this Service to harm or intimidate a minor. HomeTel complies with all federal and state laws pertaining to the protection of minors.

Spam/E-Mail/Usenet/Blog/Social-Networking Abuse:

Violation of the CAN-SPAM Act of 2003, the Electronic Mail Act of Illinois (Public Act 91-0233), or any other state or federal law regulating e-mail services, constitutes an automatic violation of this AUP and HomeTel reserves the right to seek damages and other available relief against Customer, as applicable. Spam/E-mail/Usenet Abuse is prohibited on HomeTel IP Services. Examples of Spam/E-mail/Usenet Abuse include, but are not limited to, the following activities:

- Sending unsolicited electronic mail messages and "mail-bombing" (sending mass unsolicited e-mail messages to a single user, or group of users, commercial or otherwise, or deliberately sending very large attachments to one recipient) using IP Service(s) are prohibited.
- Using another site's mail server to relay mail without the express permission of the site;
- Using another computer, without authorization, to send multiple e-mail messages or to retransmit e-mail messages for the purpose of misleading recipients as to the origin;
- Using IP addresses that the Customer does not have a right to use;
- Collecting the responses from unsolicited electronic messages;
- Maintaining a site that is advertised via unsolicited electronic messages, regardless of the origin of the unsolicited electronic messages;
- Spamming, or sending unsolicited commercial e-mail, sending unsolicited electronic messages with petitions for signatures, or any chain mail related materials, or requests for charitable donations;
- Sending messages that are harassing or malicious, or otherwise could reasonably be predicted to interfere with another party's quiet enjoyment of the HomeTel IP Services or the Internet (e.g., through language, frequency, size or otherwise);
- Sending bulk (i.e., twenty-five or more recipients) electronic messages without identifying, within the message, a reasonable means of opting out from receiving additional messages from the sender;
- Using distribution lists containing addresses that include those who have opted out;
- Sending electronic messages that do not accurately identify the sender, the sender's return address, the e-mail address of origin, or other information contained in the subject line or header:
- Forging headers or identifiers in order to disguise the origin of e-mail;
- Use of redirect links in unsolicited commercial e-mail to advertise a website or service;
- Posting a single message, or messages to online forums or newsgroups, that could reasonably be expected to provoke complaints;
- Posting messages to or canceling or superseding messages on an online forum or newsgroup in a manner that violates the rules of the forum or newsgroup or that contain forged header information;
- Sending bulk electronic messages in quantities that exceed standard industry norms, or that create the potential for disruption of the HomeTel network or of the networks with which HomeTel interconnects;
- Intercepting, redirecting or otherwise interfering or attempting to interfere with e-mail intended for other parties;
- Knowingly deleting any author attributions, legal notices or proprietary designations or labels in a file that the user mails or sends;
- Using, distributing, advertising, transmitting, or otherwise making available any software program, product, or service that is designed to violate this AUP or the AUP of any other Internet Service Provider, including, but not limited to, the facilitation of the means to spam.

Spam Damages:

Because spam related damages are often difficult to quantify, in those cases where the actual damages cannot be reasonably calculated HomeTel reserves the right to seek from the Customer liquidated damages in the amount of five dollars (US \$5.00) for each piece of 'spam' or unsolicited bulk email transmitted from or otherwise connected with Customer's account, in addition to any other rights and remedies HomeTel might have in contract, law and equity.

Commercial Use:

Customer may not resell or otherwise charge others to use the HomeTel Service. Customer agrees not to use the Service for operation as an Internet service provider, or for any other business enterprise, including, without limitation, IP address translation or similar facilities intended to provide additional access.

Security Violations:

Customer is solely responsible for the security of any device connected to the Service, including any data stored on that device. HomeTel recommends that Customer take appropriate security precautions for any systems connected to the Service. Customer is ultimately responsible for securing any wireless (WiFi) networks connected to Customer's HomeTel service. Any wireless network installed by the Customer or a HomeTel representative, that is unsecured or "open" and connected to the HomeTel network, will be deemed to be operating as an ISP and subject to the prohibition on Commercial Use set forth above. Customer authorizes HomeTel to use measures to detect unsecured wireless networks associated with your Service.

HomeTel IP Services may not be used to interfere with, to gain unauthorized access to, or otherwise violate the security of HomeTel's or another party's server, network, personal computer, network access or control devices, software or data, or other system, or to attempt to do any of the foregoing. Examples of violations of system or network security include, but are not limited to:

- Intercepting, interfering with or redirecting e-mail intended for third parties, or any form of network monitoring, scanning or probing, or other action for the unauthorized interception of data or harvesting of e-mail addresses;
- Using the Service to breach or attempt to breach the security of another user or attempt to gain access to any organization or person's computer, software, or data without the knowledge and consent of such person ("Hacking"). The equipment and the Service may not be used in any attempt to circumvent the user authentication or security of any host, network or account. This includes, but is not limited to, accessing data not intended for the Customer, logging into or making use of a server or account Customer is not expressly authorized to access, or probing the security of other networks or computers for any reason. Use or distribution of tools designed for compromising security, such as password guessing programs, cracking tools, packet sniffers or network probing tools, is strictly prohibited;
- Impersonating others in order to obtain another user's account password or other personal information;
- Using the IP Service(s) to deliver Spyware, Adware, or secretly or deceptively obtain the personal information of third parties (phishing, etc.), or engage in modem hi-jacking;
- Using any program, file, script, command or the transmission of any message or content of any kind, designed to interfere with a terminal session or the access or use of the Internet or any other means of communication;
- Distributing or using tools designed to compromise security, including cracking tools, password guessing programs, packet sniffers or network probing tools (except in the case of authorized legitimate network security operations);
- Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner of the system or network; this would include use of sniffers or SNMP tools;
- Falsifying packet header, sender, or User information whether in whole or in part to mask the identity of the sender, originator or point of origin; and
- Knowingly uploading or distributing files that contain viruses, Trojan horses, worms, time bombs, Cancelbots, corrupted files, or any other similar software or programs that may damage the operation of another's computer or property of another;
- Engaging in the transmission of pirated software, or otherwise exporting illegal software, or violating U.S. laws concerning the transmission of technical data and other regulated materials via the IP Services offered by HomeTel;
- With respect to dial-up accounts, using any software or device designed to defeat system time-out limits or to allow your account to stay logged on while you are not actively using the HomeTel IP Service(s) or using your account for the purpose of operating a server of any type;
- Using manual or electronic means to avoid any use limitations placed on the Services;
- Gaining unauthorized access to private networks;

- Violating rules, regulations, and policies applicable to any network, server, computer database, web site, or ISP that you access through the IP Service(s).

Network Usage:

No User shall excessively use Network resources on the HomeTel Network. HomeTel defines excessive usage as downloads exceeding 250 GB per month per account. Further, HomeTel reserves the right to adjust this usage limit as needed to ensure equitable use of Network capacity by other Users. HomeTel, at any time and in its sole discretion, reserves the right to disconnect any Internet Access account that causes excessive Network load or use of excessive network resources in violation of this AUP. Home Tel reserves the right to monitor the use of Network resources to ensure compliance with this policy.

Where a HomeTel Service account, service or feature description specifies limits on bandwidth, disk utilization, simultaneous connections, and/or aggregate data download or upload capacity, use in excess of those limits is not permitted without an appropriate change in account type or status, and may incur additional charges for such usage. Bandwidth, disk utilization, simultaneous connections, and aggregate data downloads/uploads will be computed or determined by HomeTel from time to time in developing its product and service offerings. In the event HomeTel determines that an account is exceeding the relevant bandwidth, disk utilization, aggregate data download/upload limits, simultaneous connections, or reasonable session times, the account owner will generally be notified by E-mail. If the excess use continues after such notification, the owner may be requested to upgrade the type of account or to modify the activity creating the excess use, or the account may be terminated. If excessive bandwidth, disk space utilization, simultaneous connections, aggregate data download or upload, or session length is determined to adversely affect HomeTel's ability to provide service, immediate action may be taken. The account owner may be notified by e-mail as soon as practical thereafter. Peak network usage is between 4 pm and 11 pm Monday – Friday and 10 am – 11 pm Saturday and Sunday. During peak usage times, priority is given to applications such as browsing, email, streaming, instant messaging, gaming and VoIP.

Congestion due to malfunctioning hardware and/or software will be remedied as quickly as network engineers can diagnose and identify the offending hardware / software. Congestion due to malice will be remedied using any technique available, including protocol-aware filtering and rate-limiting, to control and limit the offending source. HomeTel may seek criminal charges against those who inflict network malice. HomeTel may also attempt to recover costs incurred from network malice.

HomeTel will not ask you for your password in an unsolicited telephone call or email. If you believe your password has been compromised, you should immediately change your password to prevent the unauthorized use of it.

Blocking:

HomeTel shall not unjustly or unreasonably block access to lawful content, applications, services or non-harmful devices, subject to reasonable network management.

Discrimination:

HomeTel shall not unreasonably discriminate in transmitting lawful network traffic over a consumer's broadband Internet access service, subject to reasonable network management practices.

Customer Responsibilities:

Customer remains solely and fully responsible for the content of any material posted, hosted, downloaded/uploaded, created, accessed or transmitted using the IP Services. HomeTel takes no responsibility and assumes no liability for any material created or accessible on or through the HomeTel network(s) using IP Service(s), or for any mistakes, defamation, slander, libel, omissions, falsehoods, obscenity, pornography, or profanity Customer (or its Users) may encounter. As the provider of IP Service(s), HomeTel is only a forum and is not liable for any statements, representations, or content provided by the users of IP Services in any public forum. HomeTel shall not be obligated to monitor or exercise any editorial control over such material, but reserves the right to do so. In the event that HomeTel becomes aware that any such material may violate this AUP, other applicable terms of use or contract provisions, and/or expose HomeTel to civil or criminal liability, HomeTel reserves the right to block access to such material and suspend or terminate the Service of any user creating, storing or disseminating such material. HomeTel further reserves the right to conduct investigations into fraud, violations of the Terms of Service, this AUP or other laws or regulations, and to cooperate with legal authorities and third parties in the investigation of alleged wrongdoing, including disclosing the identity of the user that HomeTel deems responsible for the wrongdoing. Customer agrees to indemnify and hold HomeTel harmless from any claim, action, demand, loss, or damage (including attorneys' fees) made by any third party against HomeTel as a provider of the IP Service(s) arising out of or relating to any violation(s) of this AUP by Customer (or its Users).

Commercial Pricing

Please click on the following website link for pricing information including monthly prices, usage-based fees, and fees for early termination or additional network services: <http://www.hometel.com/internet/>.

Important Customer Information:

In addition to the terms and conditions set forth in this AUP, service is subject to the Service Agreement, which you should read carefully before activating any Service. For additional terms and conditions of Service, refer to the Service Agreement, or speak with a customer service representative by contacting them at: admin@hometel.com, 618-644-2211 or 618-651-9308.

Incident Reporting:

Any complaints (other than claims of copyright or trademark infringement) regarding violation of this AUP by a HomeTel Customer (or its User) should be directed to HomeTel's Policy Management Department. Where possible, include details that would assist HomeTel in investigating and resolving such complaint (i.e. expanded headers and a copy of the offending transmission).

Revisions to the AUP:

HomeTel reserves the right to modify its AUP at any time, and effective when posted to HomeTel's web site (<http://www.hometel.com/internet/policies/>). Notice of any change to this AUP may also be provided to a Customer via electronic mail. It is ultimately the Customer's responsibility to notify HomeTel of any change of address. Customer must respond in a timely manner to complaints concerning misuse of the Service(s) obtained from HomeTel. Failure to responsibly manage the use of the Service(s) obtained from HomeTel may be cause for termination of Service(s) to you and, depending upon the terms under which you acquired your Service(s), could lead to the imposition of early termination fees.

HomeTel Policy Management Department:

Email: admin@hometel.com

US Mail: HomeTel Policy Management Department
Attn: Rachel Stopka
501 North Douglas Street
PO Box 215,
St. Jacob, IL 62281

Phone: (618) 644-2211

Fax: (618) 644-9525

Updated: November 2011