

Access Media Holdings, LLC a/k/a “Upstream”

Internet Acceptable Use Policy

Introduction

Access Media Holdings, LLC a/k/a “Upstream” (“Access Media Holdings” or “AMH”) adopted this Acceptable Use Policy (“AUP” or “Policy”) to enhance and to protect the use of the Internet and AMH Services for all users of the Services.

Please read carefully Access Media Holdings Acceptable Use Policy. This AUP is intended to:

- promote and protect the availability, integrity, security, reliability and privacy of the systems, networks, services, and products (collectively, the "Services") of Access Media Holdings, and its subsidiaries, joint ventures, affiliates, partnerships, and any other entities controlled, or partially controlled, by Access Media Holdings;
- maintain an image and reputation of Access Media Holdings as a responsible provider of the Services; and
- encourage responsible, and discourage harmful or illegal, use of the Services and/or the Internet.

This Policy sets forth principles, guidelines, and requirements governing or affecting the use by customers and any other users (collectively, "Users") of the Services or Access Media Holdings' websites. The term "User" also includes any person visiting any of Access Media Holdings' websites, whether such person is an Access Media Holdings' customer, a visitor to a public area of our Services, or a participant in one of Access Media Holdings' promotional offerings.

Acceptance of this Policy

Your use of the Services constitutes acceptance of the terms and conditions of this Policy, as it may be modified by Access Media Holdings periodically.

Access Media Holdings wants to ensure that Users use the Services and the Internet responsibly. Access Media Holdings intends to provide customers with the best residential Internet service possible. To that end, Access Media Holdings has created this AUP. This Policy addresses allowable and acceptable uses of Access Media Holdings' High-Speed Internet service (the “Service”). The Policy is in addition to any terms, conditions and restrictions contained in the Access Media Holdings' agreements, including but not limited to its Property and/or Subscriber Agreement.

Customer Obligations

All Users must comply with this Policy. Your failure to comply with this Policy could possibly result in the termination or temporary suspension of your Services. If you do not agree to comply with this Policy, you must immediately stop all use of the Service and notify AMH so that it can close your account.

Access Media Holdings may revise this Policy from time to time by posting a new version on the Web site at <https://www.upstream.network/policies> or any successor URL(s) (Access Media Holdings' and Upstream.com Web site"). Access Media Holdings will use reasonable efforts to make customers aware of any changes to this Policy, which may include sending e-mail announcements or posting information on the Access Media Holdings Website. Revised versions of this Policy are effective immediately upon posting. Accordingly, Users of the Service should read any Access Media Holdings' announcements they receive and regularly visit the Access Media Holdings Website and review this Policy to ensure that their activities conform to the most recent version.

You can send questions regarding this Policy to, and report violations of it at <https://www.upstream.network/contact/>.

To report a child exploitation incident involving the Internet use the same link, <https://www.upstream.network/contact/>.

Allowable Uses and Activities

What uses and activities does Access Media Holdings prohibit?

The Policy prohibits uses and activities involving the Service that are illegal, infringe the rights of others, or interfere with or diminish the use and enjoyment of the Service by others and all Users. These prohibited uses and activities include, but are not limited to, using the Service, Customer equipment, or the Access Media Holdings' equipment to:

Restricted Technical Uses

- access any other person's computer or computer system, network, software, or data without his or her knowledge and consent; breach the security of another user or system; or 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 you, logging into or making use of a server or account you are not expressly authorized to access, or probing the security of other hosts, networks, or accounts without express permission to do so;
- use or distribute tools or devices designed or used for compromising security or whose use is otherwise unauthorized, such as password guessing programs, decoders, password gatherers, keystroke loggers, analyzers, cracking tools, packet sniffers, encryption circumvention devices, or Trojan Horse programs. Unauthorized port scanning is strictly prohibited;
- copy, distribute, or sublicense any proprietary software provided in connection with the Service by Access Media Holdings or any third party, except that you may make one copy of each software program for back-up purposes only;
- distribute programs that make unauthorized changes to software (cracks);
- use or run dedicated, stand-alone equipment or servers from the premises that provide network content or any other services to anyone outside of your premises local area network ("Premises LAN"), also commonly referred to as public services or servers. Examples of prohibited equipment

and servers include, but are not limited to, e-mail, Web hosting, file sharing, and proxy services and servers;

- use or run programs from the premises that provide network content or any other services to anyone outside of your Premises LAN, except for personal and non-commercial residential use;
- service, alter, modify, or tamper with the Access Media Holdings equipment or Service or permit any other person to do the same who is not authorized by Access Media Holdings.

Network and Usage Restrictions

- restrict, inhibit, or otherwise interfere with the ability of any other person, regardless of intent, purpose or knowledge, to use or enjoy the Service (except for tools for safety and security functions such as parental controls, for example), including, without limitation, posting or transmitting any information or software which contains a worm, virus, or other harmful feature, or generating levels of traffic sufficient to impede others' ability to use, send, or retrieve information;
- restrict, inhibit, interfere with, or otherwise disrupt or cause a performance degradation, regardless of intent, purpose or knowledge, to the Service or any Access Media Holdings (or Access Media Holdings supplier) host, server, backbone network, node or service, or otherwise cause a performance degradation to any Access Media Holdings (or Access Media Holdings supplier) facilities used to deliver the Service;
- resell the Service or otherwise make available to anyone outside the premises the ability to use the Service (for example, through wi-fi or other methods of networking), in whole or in part, directly or indirectly. The Service is for personal and non-commercial residential use only and you agree not to use the Service for operation as an Internet service provider or for any business enterprise or purpose (whether or not for profit);
- connect the Access Media Holdings equipment to any computer outside of your Premises;
- interfere with computer networking or telecommunications service to any user, host or network, including, without limitation, denial of service attacks, flooding of a network, overloading a service, improper seizing and abusing operator privileges, and attempts to “crash” a host; and
- access and use the Service with anything other than a dynamic Internet Protocol (“IP”) address that adheres to the dynamic host configuration protocol (“DHCP”). You may not configure the Service or any related equipment to access or use a static IP address or use any protocol other than DHCP unless you are subject to a Service plan that expressly permits you to do so.

Restricted Behavior

You may access and use the network only for lawful purposes. You are responsible for ensuring that your conduct is at all times in compliance with all applicable laws, rules, and regulations. You are responsible for any transmission you send, receive, post, access, or store via the network, including the content of any communication. transmitting, distributing, or storing any material that violates any applicable law is

prohibited. Additionally, the following non-exhaustive list details the kinds of illegal or harmful conduct that are prohibited:

- undertake or accomplish any unlawful purpose. This includes, but is not limited to, posting, storing, transmitting or disseminating information, data or material which is libelous, obscene, unlawful, threatening or defamatory, or which infringes the intellectual property rights of any person or entity, or which in any way constitutes or encourages conduct that would constitute a criminal offense, or otherwise violate any local, state, federal, or non-U.S. law, order, or regulation;
- post, store, send, transmit, or disseminate any information or material which a reasonable person could deem to be unlawful;
- upload, post, publish, transmit, reproduce, create derivative works of, or distribute in any way information, software or other material obtained through the Service or otherwise that is protected by copyright or other proprietary right, without obtaining any required permission of the owner;
- send very large numbers of copies of the same or substantially similar messages, empty messages, or messages which contain no substantive content, or send very large messages or files that disrupts a server, account, blog, newsgroup, chat, or similar service;
- Distribute, publish, or send through the network: (1) unsolicited advertisements, solicitations, commercial e-mail messages or promotional messages of any kind (commonly referred to as "spam"); (2) unsolicited informational announcements; or (3) chain mail.
- initiate, perpetuate, or in any way participate in any pyramid or other illegal scheme;
- participate in the collection of very large numbers of e-mail addresses, screen names, or other identifiers of others (without their prior consent), a practice sometimes known as spidering or harvesting, or participate in the use of software (including "spyware") designed to facilitate this activity;
- collect responses from unsolicited bulk messages;
- Online gambling is illegal in many states, and closely regulated in all states. Similarly, sweepstakes are subject to complex rules and are frequently scrutinized closely by consumer protection and law enforcement officials;
- falsify, alter, or remove message headers;
- falsify references to Access Media Holdings or its network, by name or other identifier, in messages;
- impersonate any person or entity, engage in sender address falsification, forge anyone else's digital or manual signature, or perform any other similar fraudulent activity (for example, "phishing"); and violate the rules, regulations, terms of service, or policies applicable to any network, server, computer database, service, application, system, or website that you access or use.

Network Security and Integrity

You may not violate the security of the network in any way. Such violations may result in criminal or civil liability. AMH may, but is not obligated to, investigate any violation of the network. AMH may cooperate with law enforcement where criminal or unauthorized activity is suspected. By using AMH products services or sending, receiving, posting, accessing, or storing any electronic transmission via the network, you agree to cooperate, as well, in any such investigation. Examples of network security violations include, without limitation:

- Hacking: 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 the express prior authorization of the owner of the system or network.
- Interception: Unauthorized monitoring of data or traffic on any network or system without the express prior authorization of the owner of the system or network.
- Intentional Interference: Interference with service to any user, host or network including, without limitation, denial-of-service attacks, mail bombing, news bombing, other flooding techniques, deliberate attempts to overload a system, and broadcast attacks.
- Falsification of Origin or Routing Information: Using, selling, or distributing in conjunction with the Services, any computer program designed to conceal the source or routing information of electronic mail messages in a manner that falsifies an Internet domain, header information, date or time stamp, originating e-mail address, or other identifier.
- Avoiding System Restrictions: Using manual or electronic means to avoid any limitations established by AMH or attempting to gain unauthorized access to, alter, or destroy any information that relates to any AMH customer or other end-user. AMH may, but is not obligated to, take any action it deems necessary to protect the network, its rights or the rights of its customers or third parties, or (2) optimize or improve the network, services, systems, and equipment. You acknowledge that such action may include, without limitation, employing methods, technologies, or procedures to filter or block messages sent through the network. AMH may, in its sole discretion, at any time, filter "spam" or prevent "hacking," "viruses" or other potential harms without regard to any preference you may have communicated to us.

Customer Behavior and Service Features

In addition to being responsible for your own compliance with this Policy, you are also responsible for any use or misuse of the Service that violates this Policy, even if it was committed by a friend, family member, or guest with access to your Service account. You must take steps to ensure that others do not use your account to gain unauthorized access to the Service by, for example, strictly maintaining the confidentiality of your Service login and password. In all cases, you are solely responsible for the security of any device you choose to connect to the Service, including any data stored or shared on that device. Access Media Holdings recommends against enabling file or printer sharing unless you do so in strict compliance with all security recommendations and features provided by Access Media Holdings and the

manufacturer of the applicable file or printer sharing devices. Any files or devices you choose to make available for shared access on a home LAN, for example, should be protected with a strong password or as otherwise appropriate. It is also your responsibility to secure the Customer Equipment and any other Premises equipment or programs not provided by Access Media Holdings that connect to the Service from external threats such as viruses, spam, bot nets, and other methods of intrusion.

Access Media Holdings' Assessment of Inappropriate Content and Transmissions

Access Media Holdings reserves the right to refuse to transmit or post, and to remove or block, any information or materials, in whole or in part, that it, in its sole discretion, deems to be in violation of this Policy, or otherwise harmful to Access Media Holdings' network or customers using the Service, regardless of whether this material or its dissemination is unlawful so long as it violates this Policy. Neither Access Media Holdings nor any of its affiliates, suppliers, or agents have any obligation to monitor transmissions or postings (including, but not limited to, e-mail, file transfer, blog, newsgroup, and instant message transmissions as well as materials available on the Personal Web Pages and Online Storage features) made on the Service. However, Access Media Holdings and its affiliates, suppliers, and agents have the right to monitor these transmissions and postings from time to time for violations of this Policy and to disclose, block, or remove them in accordance with this Policy, the Subscriber Agreement, and applicable law.

Electronic Mail Requirements

The Service may not be used to communicate or distribute e-mail or other forms of communications in violation of this Policy. Access Media Holdings uses reasonable network management tools and techniques to protect customers from receiving spam and from sending spam (often without their knowledge over an infected computer). Access Media Holdings is not responsible for deleting or forwarding any e-mail sent to the wrong e-mail address by you or by someone else trying to send e-mail to you. Access Media Holdings is also not responsible for forwarding e-mail sent to any account that has been suspended or terminated. This e-mail will be returned to the sender, ignored, deleted, or stored temporarily at Access Media Holdings' sole discretion. In the event that Access Media Holdings believes in its sole discretion that any subscriber name, account name, or e-mail address (collectively, an "identifier") on the Service may be used for, or is being used for, any misleading, fraudulent, or other improper or illegal purpose, AMH (i) reserves the right to block access to and prevent the use of any of these identifiers and (ii) may at any time require any customer to change his or her identifier. In addition, Access Media Holdings may at any time reserve any identifiers on the Service for Access Media Holdings' own purposes. In the event that a Service account is terminated for any reason, all e-mail associated with that account (and any secondary accounts) will be permanently deleted as well.

Instant, Video, and Audio Messages Requirements

Each user is responsible for the contents of his or her instant, video, and audio messages and the consequences of any of these messages. Access Media Holdings assumes no responsibility for the timeliness, delivery, wrong delivery, deletion, or failure to store these messages. In the event that a Service account is terminated for any reason, all instant, video, and audio messages associated with that account (and any secondary accounts) will be permanently deleted as well.

Network Management and Limitations on Data Consumption

Access Media Holdings' Management of the Network

Access Media Holdings manages its network with the goal to deliver the best possible broadband Internet experience to all of its customers. High-speed bandwidth and network resources are not unlimited. Managing the network is essential as Access Media Holdings works to promote the use and enjoyment of the Internet by all of its customers. The company uses reasonable network management practices that are consistent with industry standards. Access Media Holdings tries to use tools and technologies that are minimally intrusive and, in its independent judgment guided by industry experience, among the best in class. Access Media Holdings' network management practices will change and evolve along with the uses of the Internet and the challenges and threats on the Internet. The need to engage in network management is not limited to Access Media Holdings. Most, if not all, large Internet service providers manage their networks. Many of them use the same or similar tools that Access Media Holdings does. If Access Media Holdings did not manage its network, its customers would be subject to the negative effects of spam, viruses, security attacks, network congestion, and other risks and degradations of service. By engaging in responsible network management including enforcement of this Policy, Access Media Holdings can deliver the best possible broadband Internet experience to all of its customers.

Access Media Holdings' Management of its Network

Access Media Holdings uses various tools and techniques to manage its network, deliver the Service, and ensure compliance with this Policy and the Subscriber Agreement. These tools and techniques are dynamic, like the network and its usage, and can and do change frequently. These network management activities may include (i) identifying spam and preventing its delivery to customer e-mail accounts, (ii) detecting malicious Internet traffic and preventing the distribution of viruses or other harmful code or content, (iii) temporarily lowering the priority of traffic for users who are the top contributors to current network congestion, and (iv) using other tools and techniques that Access Media Holdings may be required to implement in order to meet its goal of delivering the best possible broadband Internet experience to all of its customers.

Restrictions on Data Consumption

The Service is for personal, residential and non-commercial use only. Access Media Holdings reserves the right to suspend or terminate Service accounts where data consumption is not characteristic of a typical residential user of the Service as determined by the company in its sole discretion. Access Media Holdings has established a monthly data consumption threshold per Access Media Holdings High-Speed Internet account of 250 Gigabytes ("GB"). Use of the Service in excess of 250GB per month is excessive use and is a violation of the Policy. Common activities that may cause excessive data consumption in violation of this Policy include, but are not limited to, numerous or continuous bulk transfers of files and other high capacity traffic using (i) file transfer protocol ("FTP"), (ii) peer-to-peer applications, and (iii) newsgroups. You must also ensure that your use of the Service does not restrict, inhibit, interfere with, or degrade any other person's use of the Service, nor represent (as determined by AMH in its sole discretion) an overly large burden on the network. In addition, you must ensure that your use of the

Service does not limit or interfere with Access Media Holdings' ability to deliver and monitor the Service or any part of its network. If you use the Service in violation of the restrictions referenced above, that is a violation of this Policy. In these cases, Access Media Holdings may, in its sole discretion, suspend or terminate your Service account or request that you subscribe to a version of the Service (such as a commercial grade Internet service, if appropriate) if you wish to continue to use the Service at higher data consumption levels. Access Media Holdings may also provide versions of the Service with different speed and data consumption limitations, among other characteristics, subject to applicable Service plans. Access Media Holdings' determination of the data consumption for Service accounts is final.

Violations of this Policy

Access Media Holdings reserves the right immediately terminate or suspend the Service account if you violate the terms of this Policy. Access Media Holdings does not routinely monitor the activity of individual Service accounts for violations of this Policy, except for determining aggregate data consumption in connection with the data consumption provisions of this Policy. In the company's efforts to promote good citizenship within the Internet community, it will respond appropriately if it becomes aware of inappropriate use of the Service. Access Media Holdings has no obligation to monitor the Service and/or the network. Access Media Holdings and its suppliers reserve the right at any time to monitor bandwidth, usage, transmissions, and content in order to, among other things, operate the Service; identify violations of this Policy; and/or protect the network, the Service and Access Media Holdings users. Access Media Holdings attempt to inform customers of inappropriate activities and give them a reasonable period of time in which to take corrective action. Access Media Holdings also prefers to have customers directly resolve any disputes or disagreements they may have with others, whether customers or not, without Access Media Holdings' intervention. However, if the Service is used in a way that Access Media Holdings or its suppliers, in their sole discretion, believe violates this Policy, Access Media Holdings or its suppliers may take any responsive actions they deem appropriate under the circumstances with or without notice. These actions include, but are not limited to, temporary or permanent removal of content, cancellation of newsgroup posts, filtering of Internet transmissions, and the immediate suspension or termination of all or any portion of the Service (including but not limited to newsgroups). Neither Access Media Holdings nor its affiliates, suppliers, or agents will have any liability for any of these responsive actions. These actions are not Access Media Holdings' exclusive remedies and Access Media Holdings may take any other legal or technical actions it deems appropriate with or without notice. In implementing this Policy, AMH shall comply with all applicable law, including regulations of the FCC. Access Media Holdings reserves the right to investigate suspected violations of this Policy, including the gathering of information from the user or users involved and the complaining party, if any, and examination of material on Access Media Holdings' servers and network. During an investigation, Access Media Holdings may suspend the account or accounts involved and/or remove or block material that potentially violates this Policy. You expressly authorize and consent to Access Media Holdings and its suppliers cooperating with (i) law enforcement authorities in the investigation of suspected legal violations, and (ii) and system administrators at other Internet service providers or other network or computing facilities in order to enforce this Policy. Upon termination of your Service account, Access Media Holdings is authorized to delete any files, programs, data, e-mail and other messages associated with your account (and any secondary accounts). The failure of Access Media Holdings or its suppliers to enforce this Policy, for whatever reason, shall not be construed as a waiver of any right to do

so at any time. You agree that if any portion of this Policy is held invalid or unenforceable, that portion will be construed consistent with applicable law as nearly as possible, and the remaining portions will remain in full force and effect. You agree to indemnify, defend and hold harmless Access Media Holdings and its affiliates, suppliers, and agents against all claims and expenses (including reasonable attorney's fees) resulting from any violation of this Policy. Your indemnification will survive any termination of the Subscriber Agreement. If You have been determined to have violated this Policy, then You will be liable to Access Media Holdings for all costs and expenses, including incidental and consequential damages, incurred by Access Media Holdings as a result of such violation. Access Media Holdings may also assess You for administrative costs and, should Access Media Holdings elect to reactivate the Services, a reactivation charge. The rights and remedies reserved by Access Media Holdings are not and are not intended to be exclusive of any other right or remedy available to Access Media Holdings at law or in equity. Each and every right and remedy shall be cumulative and in addition to any other right or remedy reserved to Access Media Holdings under this Policy or now or hereafter legally existing upon the occurrence of a violation of this Policy. The failure of Access Media Holdings at any time or from time to time to insist, or the election by Access Media Holdings at any time or from time-to-time not to insist, upon the strict observance by any User with of any provision of this Policy, shall not impair or be deemed in any way to have modified or waived Access Media Holdings' right to insist thereafter on the strict observance or performance of this Policy or any provision of this Policy. The failure of Access Media Holdings at any time or from time to time to exercise, or the election by Access Media Holdings at any time or from time to time not to exercise, any right or remedy available to Access Media Holdings as provided in this Policy, shall not impair or be deemed in any way to have modified or waived Access Media Holdings' right to exercise thereafter such right or remedy. Every right and remedy available to Access Media Holdings may be exercised at any time and from time to time and as often as may be deemed expedient by Access Media Holdings.

Copyright and Digital Millennium Copyright Act Requirements

Access Media Holdings complies with U.S. copyright and related laws, and requires all customers and Users of the Service to comply with the same laws. You may not store any material or content on, or disseminate any material or content over, the Service (or any part of the Service) in any manner that constitutes an infringement of third party intellectual property rights, including rights granted by U.S. copyright law. Owners of copyrighted works who believe that their rights under U.S. copyright law have been infringed may take advantage of certain provisions of the Digital Millennium Copyright Act of 1998 (the "DMCA") to report alleged infringements. It is Access Media Holdings' policy in accordance with the DMCA and other applicable laws to reserve the right to terminate the Service provided to any customer or User who is either found to infringe third party copyright or other intellectual property rights, including repeat infringers, or who Access Media Holdings, in its sole discretion, believes is infringing these rights. AMH may terminate the Service at any time with or without notice for any affected customer or User. Copyright owners may report potential infringements of their works that are stored on the Service or the Personal Web Features by sending Access Media Holdings' authorized agent a notification of claimed infringement that satisfies the requirements of the DMCA. Upon receipt of a probable notice of infringement, Access Media Holdings shall respond to either directly or indirectly (a) remove the allegedly infringing work(s) stored on the Service or the Personal Web Features or (b) disable

access to the work(s). AMH will also undertake commercially reasonable efforts to notify the affected customer or User of the Service of the removal or disabling of access to the work(s).

Copyright owners may send Access Media Holdings a notification of claimed infringement to report alleged infringements of their works to:

Legal @ upstream.network, 900 Commerce Drive, Suite 200, Oak Brook, IL 60523
e-mail: legal@upstream.network

Copyright owners may use their own notification of claimed infringement form that satisfies the requirements of Section 512(c)(3) of the U.S. Copyright Act. Under the DMCA, anyone who knowingly makes misrepresentations regarding alleged copyright infringement may be liable to Access Media Holdings, the alleged infringer, and the affected copyright owner for any damages incurred in connection with the removal, blocking, or replacement of allegedly infringing material.

Access Media Holdings' Network Monitoring

Access Media Holdings does not intend to actively monitor the content of websites, e-mail, news groups, or other materials created or accessible over its Services and is not responsible for the content thereof. Access Media Holdings, however, reserves the right to monitor such Services, and to take any action it deems appropriate based on information discovered in connection with any such monitoring. Access Media Holdings may investigate incidents involving alleged violations of this Policy, may cooperate with law enforcement and other third parties, and may take any action it deems appropriate based on information discovered in such investigations. User acknowledges that failure by Access Media Holdings to take action in response to any violation by any User of this Policy will not be deemed a waiver of Access Media Holdings' right to take action in response to any other violation of this Policy by that or any other User.

Investigation and Enforcement of this Policy

AMH may access and disclose any information (including transactional information) related to your access and use of the network for any lawful reason, including but not limited to: (1) responding to emergencies; (2) complying with the law (e.g., a lawful subpoena); (3) protecting Access Media Holdings' rights or property and those of its customers; or (4) protecting Users of the Services and others from fraudulent, abusive, or unlawful use of, or subscription to, such Services. Indirect or attempted breaches of this Policy, and actual or attempted breaches by a third party on behalf of a company, customer, or User, may be considered breaches of this Policy by such company, customer or User.

Warranties

ACCESS MEDIA HOLDINGS PROVIDES THE SERVICES "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED. ACCESS MEDIA HOLDINGS DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTY ARISING OUT OF USAGE OF TRADE, COURSE OF DEALING OR COURSE OF PERFORMANCE. USER IS SOLELY RESPONSIBLE FOR THE SELECTION, USE AND SUITABILITY OF THE SERVICES, AND ACCESS MEDIA HOLDINGS HAS NO LIABILITY THEREFOR. ACCESS MEDIA HOLDINGS DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED OR ERROR FREE OR THAT THEY WILL MEET USER'S

REQUIREMENTS OR PREVENT UNAUTHORIZED ACCESS. ACCESS MEDIA HOLDINGS MAKES NO WARRANTIES AND IS NOT RESPONSIBLE FOR THE CONTENT OF WEBSITES, E-MAIL, NEWS GROUPS, OR OTHER MATERIALS CREATED (OTHER THAN BY ACCESS MEDIA HOLDINGS) OR ACCESSIBLE OVER ITS SERVICES.

Limitation of Liability

IN NO EVENT WILL ACCESS MEDIA HOLDINGS BE LIABLE TO ANY USER OR THIRD PARTY FOR ANY DIRECT, INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL OR OTHER CONSEQUENTIAL DAMAGES FOR ACTIONS TAKEN OR NOT TAKEN PURSUANT TO THIS POLICY, INCLUDING, BUT NOT LIMITED TO, ANY LOST PROFITS, BUSINESS INTERRUPTION, LOSS OF PROGRAMS OR OTHER DATA, OR OTHERWISE, EVEN IF ACCESS MEDIA HOLDINGS WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE LIMITATIONS OF LIABILITY AFFORDED ACCESS MEDIA HOLDINGS HEREIN ARE IN ADDITION TO ANY LIMITATIONS SET FORTH IN ANY WRITTEN AGREEMENT BETWEEN ACCESS MEDIA HOLDINGS AND THE APPLICABLE USER ("Customer Agreement") AND WILL APPLY WHETHER THE ACTION IN WHICH RECOVERY IS SOUGHT IS BASED (A) IN CONTRACT OR TORT (INCLUDING, WITHOUT LIMITATION, NEGLIGENCE OR STRICT LIABILITY), OR (B) ON ANY LAWS.

Customer Agreements

User expressly acknowledges that nothing in this Policy will act as a limitation or be deemed a waiver of any of Access Media Holdings' rights and protections under any Customer Agreement. This Policy shall be read in concert, and not in conflict, with any such Customer Agreement. User acknowledges and agrees that this Policy, in concert with such Customer Agreement, supersedes any other oral or written representations or agreements made by AMH or its representatives regarding the Services.

Governing Law and Forum

Notwithstanding any arbitration, forum and choice of law provisions in an applicable Customer Agreement, this Policy will be governed by and interpreted in accordance with the laws of the State of Illinois, without regard to conflict of laws principles. All disputes under this Policy shall be submitted to and settled by arbitration in Cook County, Illinois, in accordance with the rules of the American Arbitration Association. The parties shall appoint a mutually agreeable arbitrator reasonably familiar with broadband communications systems and services. In the event the parties are unable to agree to a single arbitrator, the dispute shall be submitted to a panel of three (3) arbitrators, one of which shall be reasonably familiar with broadband systems and services. Each party shall appoint an arbitrator and the two arbitrators so appointed shall then select a third arbitrator. The arbitrators shall apply applicable federal laws and laws and regulations of Illinois, without regard to its choice of law principles. The decision of the arbitrators shall be binding and conclusive on all parties involved, and judgment upon their decision may be entered in a court of competent jurisdiction. The prevailing party in any such arbitration shall be entitled to collect from the non-prevailing party all costs of the arbitration, including reasonable attorneys' fees. The arbitrator shall include such award in any decision.

Severability

If any provision of this Policy, or part thereof, is held to be illegal, invalid or unenforceable by a tribunal of competent jurisdiction, then the remaining provisions, or parts thereof, shall remain in full force and effect. To the extent legally permissible, any illegal, invalid or unenforceable provision of this Policy shall

be deleted or replaced by a valid provision which will implement the purpose of the illegal, invalid or unenforceable provision.