ACCEPTABLE USE POLICY FOR
DATA STREAM RESIDENTIAL INTERNET SERVICE

Effective 05/01/2017

I. COVERAGE OF THIS POLICY

The following terms and conditions ("Policy") apply to your use of and access to Internet services ("Service") provided by Data Stream Inc. (the "Company," also referred to as "We" or "Us"), including use of or access to Company-owned or operated networks used to provide Internet services (the "Network"). This Policy outlines acceptable use of the Service, and governs your use of and access to the Service, including actions that we may take, within our sole discretion, for any use that we deem unacceptable.

This Policy is in addition to any restrictions or conditions contained in the Company's Agreement for Residential Services with you (the "Subscriber Agreement"), the Company's Privacy Policy, and any other agreements between the Company and you.

By using or accessing the Service, you agree to be bound by this Policy. If you do not wish to be bound by this Policy, you should not access, subscribe to, or otherwise use the Service and must immediately stop all use of the Service. If you violate this Policy, our remedies may include immediate suspension or termination of the Service.

II. PERMITTED AND PROHIBITED USES

A. Use must be lawful and non-harmful

You may access and use the Service only for lawful and non-harmful purposes. You are responsible for any transmission you send, receive, post, access, or store via the Service, including the content of any communication. Transmitting, distributing, or storing any material that violates any applicable law is prohibited.

Examples of prohibited illegal or harmful conduct include:

- Infringement. Infringement of intellectual property rights or other proprietary rights including, without limitation, material protected by copyright, trademark, patent, or trade secret. Infringement may result from the unauthorized copying, distribution and/or posting of pictures, logos, software, articles, musical works, and videos.
- Harmful Content. Disseminating or posting harmful content including, without limitation, viruses, Trojan horses, worms, or any other computer or other programming routines that may damage, interfere with, secretly intercept, or seize any system, program, data or personal information.
- Fraudulent Conduct. Offering or disseminating fraudulent goods, services, schemes, or promotions (such as make-money-fast schemes, chain letters, and pyramid schemes).
- Failure to Abide by Third-Party Policies. Violating the rules, regulations, or policies that apply to any third-party network, server, or computer database that you access.

- Export Violations. Violations of the Export Administration Act or the Export Administration Regulations administered by the Department of Commerce, or any similar or related applicable laws or regulations.
- Offensive Materials. Disseminating or posting material that is unlawful, libelous, defamatory, obscene, harassing, threatening, harmful, invasive of privacy or publicity rights, abusive, inflammatory, or otherwise objectionable.

B. Improper practices regarding electronic communications are prohibited

You may not distribute, publish, or send through the Service: (1) unsolicited advertisements, solicitations, or commercial e-mail messages (commonly referred to as "spam"); (2) very large numbers of copies of the same or substantially similar messages, empty messages, or messages which contain no substantive content; (3) very large messages or files that disrupt a server, account, blog, newsgroup, chat, or similar service. We do not provide "spam" filtering services.

You may not (1) participate in collecting e-mail addresses, screen names, or other identifiers of others, a practice sometimes known as "harvesting"; (2) participate in using software (including "spyware") designed to facilitate such activity; (3) collect responses from unsolicited bulk messages; (4) relay mail without the express permission of the account holder or the site; (5) 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"); or (6) allow a third-party to interrupt the Service or damage the Network or equipment used to support the Service or Network.

C. Network Security and Integrity may not be violated

You may not violate the security or integrity of the Service or Network in any way. Such violations may result in criminal or civil liability. The Company may, but is not obligated to, investigate any violation of the Service or Network. The Company may cooperate with law enforcement if criminal or unauthorized activity is suspected. You agree to cooperate in any such investigation.

You may not 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

Examples of prohibited network security or integrity 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 any attempt 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, distribution of software that contains a worm, virus, or other harmful feature, 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 any computer program designed to conceal the source or routing information of e-mail messages in a manner that falsifies an Internet domain, header information, date or time stamp, originating e-mail address, or other identifier.
- Compromising Security. Use or distribution of tools, devices, or practices 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, Trojan Horse programs, or unauthorized port scanning.
- Avoiding System Restrictions. Using manual or electronic means to avoid any limitations established by the Company or attempting to gain unauthorized access to, alter, or destroy any information that relates to any Company customer or other end-user.
- Public Server. Use or running of public servers, i.e., dedicated, stand-alone equipment or servers from your Premises that provide network content or any other services to anyone outside of your Premises local area network ("Premises LAN"). Examples include, but are not limited to, e-mail, web hosting, file sharing, and proxy services and servers; providing network content or any other services to anyone outside of your Premises LAN, except for personal and non-commercial residential use; and using the Service or Network as an Internet service provider.
- Tampering. Altering, modifying, or tampering with the Service or Network, or permitting any other person to do the same who is not authorized by Data Stream.
- Performance Degradation. Restricting, inhibiting, interfering with, or otherwise disrupting, or causing a performance degradation to, regardless of intent, purpose or knowledge, to the Service or Network or any Data Stream host, server, backbone network, node or service.
- Resale. Reselling the Service, or otherwise making available to anyone outside the Premises, the ability to use the Service (for example, through WiFi or other methods of networking), in whole or in part, directly or indirectly.
- IP Address. Accessing or using the Service or Network 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 Network 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.

The Company may, but is not obligated to, take any action it deems necessary to (1) protect the Service and 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 Service or Network. The Company 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.

III. NETWORK MANAGEMENT

The Company strives to manage the Network and the Service so as to deliver the best possible broadband Internet experience to all of its customers. The Company may use reasonable network management practices, consistent with industry standards. The Company's network management practices may change and evolve along with the uses of the Internet and the challenges and threats on the Internet. 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 as appropriate to meet the goal of delivering the best possible broadband Internet experience to all of the Company's customers.

If necessary, depending on your usage, the Company may apply data or bandwidth thresholds to the Service. Such thresholds will depend on overall Network usage and, when applied, may result in slower Service speeds.

IV. CUSTOMER OBLIGATIONS

You are responsible for your own compliance with this Policy. You are also responsible for any use or misuse of the Service that violates this Policy by anyone else you permit to access the Service (such as a friend, family member, or guest). The Company recommends against enabling file or printer sharing unless you do so in strict compliance with all security recommendations and features provided by the Company 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 Premises LAN, for example, should be protected with a strong password or as otherwise appropriate. In all cases, you are solely responsible for the security of any device you connect to the Service or Network, including any data stored or shared on that device. It is also your responsibility to secure any equipment or programs not provided by the Company that connects to the Service or to the Network from external threats such as viruses, spam, bot nets, and other methods of intrusion.

You are responsible for the contents of your e-mail, instant video and audio messages, and other communications using the Network or the Service, and the consequences of any of these communications. The Company assumes no responsibility for the timeliness, mis-delivery, deletion, or failure to store these communications. If you cancel or terminate the Service account for any reason, such communications associated with that account may be permanently deleted as well. The Company 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. The Company is also not responsible for forwarding e-mail sent to any account that has been suspended or terminated.

This e-mail may be returned to the sender, ignored, deleted, or stored temporarily at the Company's sole discretion.

V. BREACH OF THE POLICY

You are responsible for ensuring that your conduct is at all times in compliance with this Policy, and with all applicable laws, rules, and regulations.

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.

VI. INVESTIGATION, ENFORCEMENT, AND COMPANY RIGHTS

A. Monitoring the Network and Service

The Company has no obligation to monitor the Service and/or the Network, but it reserves the right to do so at any time to monitor bandwidth, usage, transmissions, and content in order to, among other things, operate the Service and Network; identify violations of this Policy; and/or protect the Network, the Service and the Company's users.

The Company generally does not exercise control over the content of information created or accessed over the Network or the Service, but reserves the right to do so in order to refuse to transmit or post, and to disclose, 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 the Network or customers using the Service.

B. Investigation and Enforcement

We have the right, but are not obligated, to strictly enforce this Policy through self-help, active investigation, litigation and prosecution. Any user that the Company determines to have violated any terms of this Policy may be subject to immediate suspension or termination of the Service, as the Company determines is reasonably practical under the circumstances to address the underlying violation. In the event that the Company becomes aware that you have violated the terms of this Policy and/or exposed the Company to civil or criminal liability including, without limitation, under the Digital Millennium Copyright Act (DMCA), the Company reserves the right to block access for, and suspend or terminate, any user creating, storing, copying, or communicating such material. The Company further reserves the right to conduct investigations into fraud, violations of the terms of this Policy 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 the Company deems responsible for the wrongdoing.

We may also access and disclose any information (including transactional information) related to your access and use of the Service or 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 our rights or property and those of our customers; or (4) protecting users of third-party

services, and third-party service providers, from fraudulent, abusive, or unlawful use of, or subscription to, such third-party services.

VII. CHANGES TO THIS POLICY

The Company may modify this Policy at any time without notice to you. Modifications will be deemed effective immediately upon posting of the modified terms at www.dtestream.com/terms. The Company 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 Data Stream website (www.dtestream.com).

VIII. COPYRIGHT / DMCA

It is a violation of this Policy to use the Service for unauthorized copying or distribution of copyrighted material. The Company reserves the right to terminate the Service, without notice, to any customer or user who is either found to infringe third-party copyright or other intellectual property rights, including repeat infringers, or who the Company, in its sole discretion, believes is infringing these rights.

IX. OTHER TERMS AND CONDITIONS

This Policy is governed by and construed under the laws of the State of Minnesota, without regard to its conflict of laws principles. The federal courts within the state of Minnesota and state courts in Hennepin County, Minnesota, have exclusive jurisdiction over and venue of any suit that relates to this Policy.

You agree to indemnify, defend and hold harmless the Company, its officers, directors, employees, agents, shareholders, licensors, and suppliers from and against all claims, liabilities, losses, expenses, damages and costs, including reasonable attorneys' fees, that arise from: (1) any violation of this Policy by you; (2) any violation of any rights of a third party by you; (3) any violation of applicable law; (4) information or content that you submit, post, transmit or make available through the Service or Network; or (5) your use of the Service or Network.

Failure by the Company to insist upon or enforce strict performance of any provision of this Policy will not be construed as a waiver of any provision or right. Neither the course of conduct between the parties nor trade practice will act to modify any provision of this Agreement. The Company may assign its rights and duties under these terms to any party at any time without notice to you. If any provision of this Policy is found to be unenforceable or invalid, this Policy's unaffected provisions will remain in effect.

You can send questions regarding this Policy to, and report violations of it, at info@dtestream.com or 888-719-2464.