



INSIGHT BROADBAND COMMERCIAL BUSINESS ACCEPTABLE USE POLICY

Insight has adopted the following Acceptable Use Policy ("AUP") to outline the proper access and usage of the InsightBusiness High Speed Broadband commercial services (the "Commercial Service"), which includes any related equipment, services or storage provided by Insight and/or through the Commercial Service. These policies and use restrictions are in addition to requirements contained in the Insight Commercial Service Agreement (the "Commercial Agreement") and any other applicable Insight terms of service or policies. Terms provided in this AUP that are not defined herein shall have the same meaning as provided in the Commercial Agreement and related terms of service.

UPDATES TO THIS AUP

Insight reserves the right to update or revise this AUP from time to time without notice. Any such update shall be effective upon the online posting of the revised AUP or otherwise making the revised AUP available for access by the Business Customer. Business Customer is responsible for ensuring that all of its authorized users and/or any others who may have access to the Commercial Services and/or Insight's network through Business Customer's Commercial Service account ("Users") have access to the limitations contained in this AUP, including any updates, prior to any Commercial Service usage. The continued use of Commercial Services following any update to this AUP evidences an agreement to be bound by the amended AUP. If you do not agree to comply with this AUP or any other Insight policies, you must immediately stop use of the Commercial Services and notify Insight.

USAGE RESPONSIBILITY

All businesses and commercial establishments that subscribe to the Commercial Service ("Business Customer(s)") and Users are required to comply with this AUP. Business Customers are responsible and liable for any failure by any Users to comply with the restrictions and limitations contained in this AUP and any other applicable Insight policies. Business Customers are also responsible for, and bear all risks associated with, any User access to the Commercial Services, any usage or transmissions occurring through the Business Customer's Commercial Service account, and for maintaining the security of the Commercial Services and any devices connected to such Commercial Services on or through Business Customer's Premises, including any data, materials, content or other information stored, transmitted, accessed or shared through such devices or equipment.

CUSTOMER'S SECURITY OBLIGATIONS

Business Customer must take steps to prevent others from obtaining unauthorized access to, or use of, the Business Customer's Commercial Services by implementing internal security protections, including, but not limited to, setting limits on User access and usage, maintaining the confidentiality of passwords or any other account or login information, protecting and/or securing open system or equipment ports, and prohibiting unauthorized access or usage of the Commercial Services and Business Customer's equipment or devices used to connect to the Commercial Service. Business Customer must establish and implement business practices for authorized end Users requiring compliance with these security protections and the limitations in this AUP. Business Customers must also maintain readily accessible contact information so that Users may notify the Business Customer of any Commercial Service issues. The Business Customer must promptly notify Insight of any Commercial Service issues or complaints.

PROHIBITED USE AND ACTIVITY

Business Customers are responsible for any transmissions sent, received, accessed, posted or stored via the Commercial Services subscribed to by the Business Customer, including any content of transmissions or communications. Business Customers and Users are expressly prohibited from accessing or using the Commercial Services in violation of any Prohibited Use. Prohibited Uses include, but are not limited to, using the Commercial Services or any related Equipment or connected devices to engage in any activity that:

- i. **Violates any law, rule or regulation.** The uploading, posting, storing, reproducing, transmitting, disseminating, or otherwise publishing information, data, content, software, code or material which is libelous, obscene, threatening, harassing or defamatory; violates the privacy or publicity rights of others; or which in any way constitutes, encourages conduct that would constitute, or facilitates a criminal offense, gives rise to civil liability, or otherwise violates any local, state, federal or international law, order or regulation.

ii. **Offends other persons.** The posting, storing, transmitting or dissemination of any information, content, software, or material which a reasonable person could deem to be offensive, indecent, pornographic, harassing, distressing, vulgar, hateful, inflammatory, racially or ethnically offensive or otherwise objectionable, regardless of whether such material or its dissemination is unlawful.

iii. **Interferes with or compromises security measures.** The accessing or attempting to access or breach any other person's computer, electronic device, software, code, data, transmissions or content without their knowledge and/or consent; attempting to circumvent the user authentication or security of any host, network, or account by accessing data, code or any other information not intended to be made accessible to another person; logging into or making use of a server or account that you are not expressly authorized to access; or probing or scanning the security or ports of other Internet users, devices or networks outside the Business Customer's premises. These prohibitions also preclude the use or distribution of tools designed or used for compromising the security of the Commercial Services, Insight's network, Equipment or other Insight services, including, but not limited to, viruses, worms, time bombs, password guessing programs, decoders, password gatherers or cracking tools, encryption circumvention devices, or other programs that may damage, interfere with, secretly intercept or seize any system program, data or personal information without authorization.

iv. **Harms or attempts to harm minors.** The use of, or allowing others to use, the Commercial Services in any way to harm or attempt to harm a minor, including, but not limited to, using the Commercial Services to access, post, store, transmit or disseminate minor pornography or obscene, indecent, graphic or profane materials involving a minor.

v. **Infringes the intellectual property rights of any person or entity.** The uploading, downloading, posting, storing, publishing, transmitting, reproduction, creation of derivative works of, or the distribution in any way of information, software, code, content or other material through the Commercial Service which is protected by copyright, patent, trademark or other proprietary right, without having permission of the owner or other right to such use under applicable law (whether through direct or contributory infringement, or inducement to infringe).

vi. **Interferes with Commercial Service performance or usage by other persons.** Restricting, inhibiting, interfering or otherwise interrupting, disrupting or causing performance degradation, regardless of intent, purpose or knowledge, to the Commercial Services; any Insight (including Insight supplier or vendor) host, server, network, node or service; any other facilities used to provide or deliver the Commercial Services; or to the ability of any person to access, use or enjoy any Insight service. Such interferences or disruptions include, but are not limited to, denial of service attacks, overloading or flooding the system, allowing or facilitating use of the Commercial Service in a manner that exceeds the number of authorized Users or amount of storage for an account, or other activity that disrupts or otherwise interferes with authorized Commercial Service bandwidth, data storage, security or other Commercial Service features. This prohibition precludes the connection of any Business Customer equipment or device, by any means, to the Commercial Services that may cause any of the above disruptions or otherwise violate this AUP.

vii. **Resells or distributes the Service in violation of your Commercial Agreement and related terms of service.** The resale of any portion of the Commercial Services, redistributing the Commercial Services, offering any Commercial Service feature to others as a service or feature of the Business Customer's business, or otherwise making the Commercial Service available to anyone outside the Business Customer's premises who is not an authorized User through either intentional actions or failure to implement and maintain proper security in a manner that violates the Commercial Agreement and related terms of service. Business Customer may share authorized Commercial Services or access with Business Customer approved Users or contractors via a LAN, VPN or other remote access method as long as such access and usage does not violate this AUP or the Commercial Agreement. Business Customer shall not use, share or otherwise make available, or allow others to use or share the Commercial Service for operation as an Internet Service Provider, host or service bureau, whether or not for compensation or pecuniary gain, unless expressly authorized by written agreement with Insight. The Commercial Service is intended and may only be used for business purposes by the Business Customer and its authorized Users within the Business Customer's premises unless otherwise authorized by written agreement with Insight.

viii. **Transmits or causes the distribution of SPAM.** Any commercial transmissions, mailings or messages must be in accordance with applicable law, including the CAN-SPAM Act, must not be considered "unsolicited SPAM" or chain mail, and must not otherwise violate the Commercial Agreement and related terms of service. Business Customers may forward, transmit or distribute lawful bulk commercial

transmissions to intended recipients for Customer's business purposes, including for advertising or promotion of the Business Customer's business, when such recipients have authorized any such contact from the Business Customer.

ix. **Exceeds Commercial Service bandwidth or other capacity limitations.** Insight may provide Commercial Service versions with different speeds, storage, bandwidth capacity or other accessible features. You may not exceed the amount of speed, storage or bandwidth purchased and authorized by the terms of your Commercial Service plan. Insight shall have the right to determine, in its sole discretion, whether Business Customer has violated the limitations of a Commercial Service plan.

x. **Provides unauthorized services to others.** The running of programs, servers or other equipment from the Business Customer's Premises that provides content, internet access or any other Insight services to others outside your authorized Users, Commercial Service Premises or Business LAN, unless such activity is authorized pursuant to your Commercial Agreement or level of subscribed Commercial Service.

xi. **Tampers with the Commercial Services or Insight Equipment.** Modifying or tampering with the Commercial Services or Insight Equipment used in the provision of Commercial Services, or permitting any unauthorized person to service, access, modify or tamper with the Insight Equipment, without written authorization by Insight.

xii. **Solicits illegal activity.** Initiating, perpetuating, or in any way participating in any pyramid or other illegal soliciting scheme, encouraging others to accept fraudulent offers, or conducting any unlawful lottery or gambling activity.

xiii. **Harvests identifiers without authorization.** The facilitating of, or participating in, collecting identifiers of others without their prior express consent, including collecting responses from unsolicited messages or using any facilities of Insight or other services to relay mail without the express permission of the account holder, site or service.

xiv. **Fraudulently misrepresents the truth.** This includes the impersonation of any person or entity, engaging in address falsification, using an IP address or client Id not assigned to you, forging any other person's digital or manual signature, misleading or misrepresenting a User's true identity, or performing any other similar fraudulent activity. This section is not intended to prevent use of authorized screen or feature names while accessing the Commercial Services or participating in online activities, chat rooms or message boards.

xv. **Violates the policies of other third parties.** Any policies set forth by another service provider or other third parties accessed through the Commercial Services must be strictly adhered to.

CUSTOMER'S CONTENT AND STORAGE OBLIGATIONS

As part of the subscribed Commercial Service, Insight may provide the ability to create and/or store content, code or business information through a service offering. Business Customer is solely responsible for, and shall bear full risk of loss, omission and/or damage to, all content, code, business information or other material that a Business Customer or User posts, stores, uploads or otherwise transmits through the Commercial Service. Any such content, code or business information must also comply with all applicable laws and not otherwise violate this AUP. Business Customer shall not use the Commercial Service as an instrument for placing or storing archived files and/or material that can be downloaded through other websites.

CONSEQUENCES FOR AUP VIOLATIONS

Failure to comply with this AUP could lead to the removal of content, materials or other information posted, stored or transmitted via the Commercial Service; limitations on Commercial Service access; reclassification of the Commercial Services; or the suspension or termination of the Business Customer's account, in addition to any other remedies available to Insight. Some additional remedies may include, but are not limited to, the recovery of costs, fees or expenses associated with (i) investigation into AUP violations; (ii) response to complaints, subpoenas or other legal process; (iii) breach or system recovery; (iv) migrating Business Customer to a higher Commercial Service level; (v) disconnection and/or removal of Commercial Services; or (vi) any other activity Insight may undertake due to an AUP violation. Insight has the sole discretion and right to determine if certain conduct violates this AUP.

Insight reserves the right to investigate suspected violation of this AUP. Insight may also cooperate with legal authorities and/or third parties in such investigation or of any suspected or alleged crime or illegal activity. You agree to cooperate with any reasonable investigation into suspected violations of this AUP or illegal activity.

Any unauthorized access or usage of the Commercial Services or any violation of this AUP relieves Insight of any obligations it may have to the Business Customer. Insight prefers to advise Business Customers of any suspected AUP violations. However, depending on the suspected violation or activity, Insight reserves the right to act immediately and without Business Customer notice to comply with legal process or to prevent, impede or stop the violation or activity to protect the Commercial Services, Insight's network and/or other persons or entity. Neither Insight nor its affiliates will have any liability for taking such responsive action.

If a Business Customer's account is suspended or terminated, Insight is authorized to delete any material, postings, content, code, pending transmissions, files, email messages and other information associated with the account. Insight may also delete any above items pursuant to its service retention policies.

VIOLATION REPORTING

Any complaints involving a violation of this AUP should be promptly reported to Insight. The complaint should include valid contact information and information that would assist Insight in identifying, investigating and resolving the complaint. Complaints concerning copyright infringement must be directed to our Copyright Agent in accordance with Insight's Policies for Considering Copyright Infringement Claims.

USAGE DISCLAIMER

Insight has no obligation to monitor the Commercial Services for authorized access and usage. We also do not exercise editorial control over any content, transmissions or other activity occurring via the Business Customer's Commercial Services. Insight disclaims all responsibility and liability for any access or use of the Commercial Services or any violation of this AUP, including any liability to a person or party due to any other person or party's violation of this AUP.

Nevertheless, we reserve the right, but do not assume the obligation, to review or monitor usage of the Commercial Services, including bandwidth capacity, transmissions and/or content, and to remove any material, transmissions or content or Commercial Service access to ensure that a Business Customer's account activity (i) adheres to this AUP and other Insight service requirements; (ii) does not improperly restrict, degrade or compromise the integrity or security of Insight's network and its ability to offer and/or deliver Commercial Services or other Insight services; (iii) does not potentially harm other Insight Customers or users; and (iv) does not violate applicable law or subject Insight to liability.

Insight is not responsible for transmissions, storage or emails, including transmissions sent to the wrong email address or to a suspended or terminated account. Such transmissions or emails may be returned to the Business Customer's account, ignored, deleted or temporarily stored by Insight.

INDEMNIFICATION

In addition to any indemnification provided in the Commercial Agreement and any related terms of service, Business Customer agrees to indemnify, defend and hold harmless Insight, as defined in the Commercial Agreement, and its affiliates against all claims, demands, costs, expenses and fees (including reasonable attorney fees and any costs or fees for investigation of such claims or demands) resulting from (i) a Business Customer and/or User engaging in any of the Prohibited Uses or other violation of this AUP, (ii) a third party's violation of this AUP when the violation occurs through the Business Customer's account or through devices or equipment on the Business Customer's Premises, (iii) violation by Business Customer or Users of any other Insight policies related to the Commercial Services, or any other third party policies. This indemnification will survive following termination of the Commercial Agreement with the Business Customer.

NO WAIVER

The failure of Insight to enforce any provision in this AUP shall not be construed as a waiver of the right to do so at any time. You agree that if any portion of this AUP is held invalid or unenforceable, that portion will be construed consistent with applicable law as close as possible, and all remaining provisions will remain in full force and effect.

COPYRIGHT CLAIMS

INSIGHT POLICIES FOR CONSIDERING COPYRIGHT INFRINGEMENT CLAIMS MADE TO INSIGHT BROADBAND SM SERVICES.

i. Copyright Claims. Insight requires the Complaining Party to substantiate a copyright claim involving our Insight Broadband Services and/or websites by providing notice to Insight in accordance with the then current

statutory requirements imposed by the Digital Millennium Copyright Act of 1998 ("DMCA"). The notice must be submitted in writing to:

Designated Agent: Sherman Hand, Manager of Security.

Postal Mail Address:
Insight Midwest, L.P.
10200 Linn Station Road
Louisville, KY 40223

Telephone Number: (502) 410-7145

Facsimile Number: (502) 410-7101

E-mail Address: dmca@insightbb.com

ii. Procedure. Upon receipt of a notice meeting the DMCA requirements, we will take such action as is appropriate under the DMCA. This may include forwarding the Complaining Party's written notification to the alleged infringer and removing or disabling access to material claimed to be infringing. In addition, we have adopted a policy where we may, in circumstances that we in our discretion deem appropriate, terminate the accounts of Insight Customers who are repeat infringers of copyrighted works, trademarks or any other intellectual property.

iii. Counter Notification. An alleged infringer who disagrees with the removal or disabling of access to materials may provide a Counter Notification by providing a written communication to Insight's Designated Agent identified in Section I above. See 17 USC Section 512 for counter-notice requirements.

Last Updated April 2007