



## **INSIGHT BROADBAND COMMERCIAL ENTERPRISE ACCEPTABLE USE POLICY**

Insight has adopted the following Acceptable Use Policy (“AUP”) to outline the proper access and usage of the Insight Broadband Commercial Enterprise Services, including the Insight high-bandwidth connectivity and any related equipment and services (collectively referred to as “Network Services”), provided to the Network Customer (also referred to as “you” or “your”). These policies and use restrictions are in addition to requirements contained in the Insight Network Services Contract (the “Network Agreement”), the Insight Broadband Commercial Service Agreement For Wireless Local Area Network Use (the “Wireless Network Agreement”) and any other applicable Insight policies. Terms provided in this AUP that are not defined herein shall have the same meaning as provided in the Network Agreement and/or the Wireless Network Agreement, as applicable.

### **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 made available for access by the Network Customer, and is available for review at [www.insightbusiness.com](http://www.insightbusiness.com) or at such other address as Insight may specify by posting or email notice. Network Customer is responsible for ensuring that all of its authorized users, customers and/or any others who may have access to the Network Services and/or Insight’s network through Customer’s Network (“Users”) have access to the limitations contained in this AUP, including any updates, prior to any Network Service usage. The continued use of Network 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 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 Network Services and notify Insight.

### **USAGE RESPONSIBILITY**

All Network Customers and Users are required to comply with this AUP. Network 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. Network Customers are also responsible for, and bear all risks associated with, any User access to the Network Services, any usage or transmissions occurring through the Customer’s Network, and for maintaining the security of the Network Services and any devices connected to the Network Services on or through 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**

Network Customer must take steps to prevent others from obtaining unauthorized access to, or use of, the Customer’s Network Services by implementing Network Service 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 Network Services and Customer Premises Equipment. Network Customer must establish and implement business practices for authorized end Users requiring compliance with these security protections and the limitations in this AUP. Network Customers must maintain readily accessible contact information so that Users may notify the Network Customer of any complaints or Network Service issues. The Network Customer must promptly notify Insight of any Network Service issues or complaints regarding the Network Services.

### **PROHIBITED USE AND ACTIVITY**

Network Customers are responsible for any transmissions sent, received, accessed, posted or stored via the Network Services installed on Customer’s Premises, including any content of transmissions or communications. Network Customers and Users are expressly prohibited from accessing or using the Network Services in violation of any Prohibited Use. Prohibited Uses include, but are not limited to, using the Network Services or Network Equipment to engage in any activity that:

- i. **Violates any law, rule or regulation.** The uploading, posting, storing, reproducing, transmitting, disseminating 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. **Interferes with or compromises security measures.** The accessing or attempting to access or breach any computer, electronic device, software, code, data, transmissions or content without consent; attempting to circumvent the user authentication or security of any host, network (including the Network Services), 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 networks. These prohibitions also preclude the use or distribution of tools designed or used for compromising the security of the Network Services, Insight's Network, Equipment or other Insight services, including, but not limited to, viruses, worms, time bombs, password guessing programs, decoders, password gatherers, encryption circumvention devices, or other programs that may damage, interfere with, secretly intercept or seize any system program, data or personal information without authorization.

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

iv. **Infringes the intellectual property rights of any person or entity.** The uploading, downloading, posting, publishing, transmitting, reproduction, creation of derivative works of, or the distribution in any way of information, software, code, content or other material 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).

v. **Interferes with Network Service performance.** Restricting, inhibiting, interfering or otherwise interrupting, disrupting or causing performance degradation, regardless of intent, purpose or knowledge, to the Network Services or any Insight (including Insight supplier or vendor) host, server, network, node or service, or to any other facilities used to provide or deliver the Network Services. This prohibition precludes the connection of any Customer Premises Equipment, by any means, to the Network Services that may cause any of the above disruptions or otherwise violate this AUP.

vi. **Resells or distributes the Service in violation of your Network Agreement or Wireless Network Agreement, as applicable.** The resale of Network Services, redistributing the Network Services, or otherwise making the Network Service available to anyone outside the Network Premises through either intentional actions or failure to implement and maintain proper security in a manner that violates the Network Service Agreement. Network Customer may share authorized Network Services or access with 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 Network Agreement or Wireless Network Agreement, as applicable.

vii. **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 Network Agreement or Wireless Network Agreement, as applicable. Network Customers may forward, transmit or distribute bulk commercial transmissions to intended recipients for Customer's business purposes, including for advertising or promotion of the Network Customer's business, when such recipients have authorized any such contact from the Network Customer.

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

ix. **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.

x. **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.

xi. **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 Network Services or participating in online activities, chat rooms or message boards.

#### **CONSEQUENCES FOR AUP VIOLATIONS**

Failure to comply with this AUP could lead to limitations on Network Service access; reclassification of the Network Services; or the suspension or termination of the Network 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) disconnection and/or removal of Network Services; or (v) 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 Network Services or any violation of this AUP relieves Insight of any obligations it may have to the Network Customer. Insight prefers to advise Customers of any suspected AUP violations. However, depending on the suspected violation or activity, Insight reserves the right to act immediately and without Network Customer notice to comply with legal process or to prevent, impede or stop the violation or activity to protect the Network Services, Insight's network and/or other persons or entity. Neither Insight nor its affiliates will have any liability for taking such responsive action.

#### **VIOLATION REPORTING**

Any complaints involving a violation of this AUP should be promptly reported to Insight.

#### **USAGE DISCLAIMER**

Insight has no obligation to monitor the Network Services for authorized access and usage. We also do not exercise editorial control over any content, transmissions or other activity occurring via the Customer's Network Services. Insight disclaims all responsibility and liability for any access or use of the Network 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 Network Services, including bandwidth capacity and transmissions, and to remove any transmissions or Network Service access to ensure that a Network Customer's account activity (i) adheres to this AUP; (ii) does not improperly restrict, degrade or compromise the integrity or security of Insight's network and its ability to offer and/or deliver Network 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.

#### **INDEMNIFICATION**

In addition to any indemnification provided in the Network Agreement or Wireless Network Agreement, as applicable, Customer agrees to indemnify, defend and hold harmless Insight and its affiliates, as defined in the Network Agreement or Wireless Network Agreement, as applicable, 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 Network 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 Customer Premises Equipment or to the Network Services on or through Customer's Premises, (iii) violation by Network Customer or Users of any other Insight policies related to the Network Services. This indemnification will survive following termination of the Network Agreement or Wireless Network Agreement, as applicable with the 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<sup>SM</sup> 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](mailto: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