800 central Parkway E
Suite 300 | Plano, TX 75074
www.trusti2i.com | 972-423-5110

Acceptable Use Policy

ATTENTION! THE FOLLOWING ACCEPTABLE USE POLICY WILL BE LEGALLY BINDING ON CUSTOMER UPON EXECUTION OF THE i2i SUBSCRIPTION SERVICES AGREEMENT ("Agreement") AND APPLICABLE STATEMENT OF WORK ("SOW"). CUSTOMER SHOULD CAREFULLY READ THE FOLLOWING **BEFORE** EXECUTING THE AFORMENTIONED AGREEMENTS.

The i2i Acceptable Use Policy ("AUP"), as amended, modified or supplemented from time to time, as set forth in the Resources Section of the website of i2i, is designed to (i) protect i2i's Customers, users of i2i's website, Products and Services, i2i's Network and physical infrastructure and third parties, (ii) further comply with all relevant laws and regulations, (iii) promote the security and availability of i2i's website, the i2i Network and physical infrastructure and (iv) regulate and restrict the use of all products and services including, but not limited to, the Products and Services provided by i2i, its website, the i2i Network and its physical infrastructure ("i2i Services").

The i2i AUP applies to all Users that subscribe for i2i Services ("Customers"), all Users who are Customers of i2i Customers ("Third Party Users"), all Users that access or utilize i2i's Website, Facilities, Network Environment and Computing Environment ("General Users"), and every server or network device that is under each User's control and attached to the i2i Network or Computing Environment as a part of i2i Services ("Server"). The term "User" hereinafter refers to Customers, Third Party Users and General Users alike.

Use of i2i's Website, Facilities, Network Environment, Computing Environment, and Services (collectively, "Services" and each a "Service") is subject to a signed Subscription Services Agreement and applicable SOW(s) between the customer and i2i and the Customer's acceptance and compliance with i2i's Service Level Agreement ("SLA), Privacy Statement, Terms and Conditions and this Acceptable Use Policy ("AUP"), each of which is incorporated herein by reference and made a part hereof (collectively, the "Agreement").

i2i HEREBY RESERVES THE RIGHT TO AMEND, ALTER, MODIFY, REPLACE OR SUSPEND FROM TIME TO TIME, AND IN ITS SOLE DISCRETION, ALL OR ANY PORTION OF i2i's TERMS AND CONDITIONS, ACCEPTABLE USE POLICY ("AUP") OR PRIVACY STATEMENT, AVAILABLE FOR REVIEW AND PRINT IN THE RESOURCE SECTION AT www.trusti2i.com. USE OF i2i's WEBSITE, FACILITIES, NETWORK ENVIRONMENT, COMPUTING ENVIRONEMENT AND SERVICES, AFTER CHANGES TO THESE DOCUMENTS ARE POSTED ON i2i'S WEBSITE, WILL CONSTITUTE THE CUSTOMER'S ACCEPTANCE OF ANY SUCH AMENDMENTS OR MODIFICATIONS.

Customers are responsible for complying with the i2i AUP, and for violations attributable to their Customers and users will comply with the i2i AUP.

The i2i AUP does not (a) obligate i2i to monitor, review, or police the data and content residing on i2i's Network or (b) create any obligation or duty of i2i to any party that is not a Customer, including, but not limited to, any Third Party User. Unless and until notified, i2i is not likely to be aware of any violations of the i2i AUP or any violations of law. i2i expects all Users to notify us of any violations of law or violations of the i2i AUP. i2i **EXPRESSLY DISCLAIMS ANY LIABILITY FOR THE DATA AND CONTENT TRANSMITTED THROUGH OR INTERMEDIATELY, TEMPORARILY OR PERMANENTLY STORED ON i2i NETWORK OR ANY SERVER AND FOR THE ACTIONS OR OMISSION OF USERS**.

1) Users' Security Obligation

Users must use reasonable care to ensure the security of each Server, i2i Network and its physical infrastructure. Customer is solely responsible for any intrusions into, or security breaches of, any of its Servers, except as otherwise covered by a specifically designated security administration or firewall security service package ordered by the Customer. i2i reserves the right to disconnect without refund or the provision of service credit any Servers which disrupt the i2i Network or any hardware objects on the Network as a result of a security compromise.

2) Prohibited Content

a) Users shall not allow the posting, transmission, or storage of data or content on or through i2i Services, the i2i Network or its physical infrastructure which, in i2i's sole determination, constitutes a violation of any federal, state, local or international law, regulation, ordinance, court order or other legal process ("Applicable Law"). Users shall be responsible for determining which Applicable Laws are applicable to their use of i2i Services. Prohibited content includes, without limitation, (a) content or code that facilitates any violation of, or describes

ways to violate, the i2i AUP or (b) "harvested" addresses or information, (c) "phishing" websites, or (d) "spamvertising" sites.

b) A User shall not knowingly use i2i Services to display or disseminate over the i2i Network, images classified under U.S. law as child pornography, child erotica (regardless of literary or artistic merit) and/or bestiality. In addition to any other actions it may take under the i2i AUP, i2i reserves the right to cooperate fully with any criminal investigation of content located on a Server that constitutes alleged child pornography or an alleged violation of Applicable Law.

3) Prohibited Activities

a) Hack, and/or subvert, or assist others in subverting, the security or integrity of the i2i Network, Products and Services;
b) Solicit the performance of any illegal activity, even if the activity itself is not performed;
c) Threaten bodily harm, or encouraging bodily harm or property destruction;
d) Harass another, or encourage harassing behavior;
e) Engage in outright fraud, or use services to engage in scams like pyramid schemes;
f) Collect personal information about others without their knowledge or consent;
g) Instruct others in prohibited activities;
h) Act in any manner that might subject i2i to unfavorable regulatory action, subject i2i to any liability for any reason;
i) Act in any manner that might adversely affect i2i's public image, reputation or goodwill, as determined by i2i in its sole and exclusive discretion

4) Anti-Spamming Policy - Users must comply with all relevant legislation and regulations on bulk and commercial e-mail, including the CAN-SPAM Act of 2003. Users shall not:

a) Send unsolicited "mass mailings" or "bulk e-mail messages known as "Spam", which is email that is sent to recipients who have not Confirmed Opt-In or Closed-Loop Opt-In in to mailings from the User.
   i) Users who send mass mailings must maintain complete and accurate records of all consents and opt-ins and provide such records to i2i upon its request.
   ii) If a User cannot provide positive and verifiable proof of such consents and opt-ins, i2i will consider the mass mailing to be unsolicited
b) Operate mailing lists, listservs, or mailing services that do not target an audience that has voluntarily signed up for e-mail information using a Confirmed Opt-In or Closed-Loop Opt-In process or that has made their e-mail addresses available to a User for distribution of information.
   i) Users who operate mailing lists must maintain complete and accurate records of all consents and Confirmed Opt-In or Closed-Loop Opt-In elections and provide such records to i2i upon its request
   ii) If a User cannot provide positive and verifiable proof of such consents and Confirmed Opt-In or Closed-Loop Opt-In elections, i2i will consider the list mailing to be unsolicited
   iii) Any User-maintained mailing list must also allow any party on the list to remove itself automatically and permanently.
c) Create fake weblog or weblogs which are intended or reasonably likely to promote the author's affiliated websites or to increase the search engine rankings of associated sites (i.e., "splogs")
d) Send spam to weblog sites or automatically post random comments or promotions for commercial services to weblogs (i.e., "spamming blogs")

i2i will not be held responsible for Customer domains being blocked by ISP's for sending out spam mail. i2i reserves the right to cancel or suspend any Customer sending out spam or unwanted email either knowingly or unknowingly. i2i may limit the number of outgoing messages to 250 per individual mailbox.

5) Prohibited Email Activities - Prohibited email activities include, without limitation, the following:

a) **Sending UCE/UBE, also known as SPAM -** Defined as the sending of email to recipients who consider the message unsolicited email of a commercial nature or the sending of email in bulk to recipients who consider the message unsolicited email of any nature
b) **Collecting UCE or SPAM Responses -** Defined as the collection of responses, directly or indirectly, from UCE or UBE sent by you or UCE or UBE sent on your behalf
c) **Spamvertising**

Acceptable Use Policy

i) Web Site Advertising via UCE or UBE **-** Defined as the sending of email which: 1) is UCE or UBE as defined above; and 2) contains direct or indirect links or references to one or more web sites. This also includes the use of third-party email accounts, servers or services to spamvertise the site(s)
ii) Hosting web pages advertised within "spam e-mail" sent from another network providing services that support spam.

d) **Flood or Mail Bombing -** Defined as the sending of an unreasonably large number of electronic mail messages to a single system, person or email address
e) **Spoofing** - Defined as forging, misrepresenting, omitting or deleting message headers, return mailing information, or internet protocol addresses to conceal or misidentify the origin of a message.
f) **Mail Harassment -** Defined as sending email in a manner or with content that is perceived as threatening or harassing by the intended or actual recipient.
   i) **Letter Bombing -** Defined as sending email with content that will or could potentially harm the recipient's computer.
   ii) **Bulk Email -** Customers with intentions to send BULK EMAIL to a list of email addresses should use an external mailing list service provider such as Constant Contact or iContact. i2i's services are not intended for this purpose and use of i2i's services in this manner is in direct violation of the SPAM policy outlined within this agreement.
g) Creating or sending Internet viruses, worms or Trojan horses, or engaging in denial of service attacks
h) Spamming via third-party proxy, aggregation of proxy lists, or installation of proxy mailing software.
i) Configuration of a mail server to accept and process third-party messages for sending without user identification and authentication.
j) Creating or sending any other unsolicited bulk messages, postings, or transmissions through media such as weblog posts, IRC/chat room messages, guestbook entries, HTTP referrer log entries, UseNet posts, pop-up messages, instant messages, or SMS messages.

If any Customer or any Third Party User that is a Customer of our Customer uses i2i Services, the i2i Network or its physical infrastructure in a manner that causes i2i to be "blacklisted" or blocked, i2i reserves the right to (i) suspend permanently or terminate i2i Services of such Customer and/or (ii) suspend permanently or terminate the access to i2i Services, i2i Network or its physical infrastructure by such Third Party User. Operating i2i Services on behalf of, or in connection with, or reselling any service to persons or firms listed in the Spamhaus Register of Known Spam Operations database at www.spamhaus.org shall constitute a violation of the i2i AUP.

6) Block Removal - If, as a result of a Customer's actions, i2i's mail servers or IP address ranges are placed on black hole lists or other mail filtering software systems, i2i shall charge Customer $100 upfront and $100 per hour thereafter for any necessary remedial actions.

7) IP Allocation - i2i owns each IP address that it assigns to a Customer. A Customer shall not use IP addresses that were not assigned to it by i2i. i2i reserves the right to suspend the network access of any server utilizing IP addresses outside of the assigned range.

8) IRC Policy - Customers may not operate and maintain IRC servers which connect to global IRC networks such as Undernet, EFnet and DALnet. Use of IRC plug-ins, scripts, add-ons, clones or other software designed to disrupt or deny service to other users is prohibited. Harassing or abusive IRC activity is expressly prohibited under the i2i AUP, including (i) disruption or denial of service or (ii) the use or joining of "botnets" or the use of IRC BNC's or other proxy and re-direction software. If a Customer's IRC servers are frequently compromised or attract denial of service or distributed denial of service attacks that disrupt or denies service to other Customers or users, i2i may null-route, filter, suspend, or terminate that Customer's service.

9) Usenet Policy - Usenet posts and content must conform to standards established by the Internet community and the applicable newsgroup charter. i2i reserves the right to determine whether such posts violate the AUP.

10) Network Abuse - Users are prohibited from engaging in any activities that i2i determines, in its sole discretion, to constitute network abuse, including, but not limited to, the following:

Acceptable Use Policy

a) Introducing or executing malicious programs into any network or server, such as viruses, worms, Trojan Horses, and key loggers
b) Causing or initiating security breaches or disruptions of network communication and/or connectivity, including port scans, flood pings, email-bombing, packet spoofing, IP spoofing, and forged routing information
c) Executing any form of network activity that will intercept data not intended for the Customer's server
d) Evading or circumventing user authentication or security of any host, network or account, including cracking, brute-force, or dictionary attacks.
e) Interfering with or denying service to any user, host, or network other than the Customer's host, such as a denial of service attack or distributed denial of service attack.
f) Conduct designed to avoid restrictions or access limits to specific services, hosts, or networks, including the forging of packet headers or other identification information.
g) Soliciting the performance of any illegal activity, even if the activity is not performed.
h) Using any program, or sending messages of any kind, designed to interfere with or disable a user's terminal session.

11) Intellectual Property Infringement Policy - Users may not transmit, distribute, download, copy, cache, host, or otherwise store on a Server, i2i Network or its physical infrastructure any information, data, material, or work that infringes the intellectual property rights of others or violates any trade secret right of any other person. i2i has the right to disable access to, or remove, infringing content to the extent required under any law or regulation, including the Digital Millennium Copyright Act of 1998. For your convenience, information concerning procedures for making claims of copyright infringement for purposes of Title 17, Section 512, of the United States Code is contained in the Resource section of i2i's website.

If any Customer or any Third Party User, including those that are Customers of our Customers, repeatedly violates i2i's Intellectual Property Infringement Policy, any copyright law or any other intellectual property right, i2i reserves the right to (i) suspend permanently or terminate i2i Services of such Customer and/or (ii) suspend permanently or terminate the access to i2i Services, i2i Network or its physical infrastructure by such Third Party User.

12) Legal Investigations - Users will cooperate and comply with any civil or criminal investigation regarding use of i2i Services, i2i Network or its physical infrastructure or content located on its Servers or transmitted using i2i Services, i2i Network or its physical infrastructure, including, without limitation, the following: discovery orders, subpoenas, freeze orders, search warrants, information requests, wire taps, electronic intercepts and surveillance, preservation requests, and any other order from a court, government entity or regulatory agency (each an "Investigation"). i2i may charge a User or any person seeking compliance with an Investigation for the reasonable costs and expenses associated with i2i's compliance with any Investigation. **i2i reserves the right to comply with any Investigation without notice to a User. Customers shall not be entitled to a refund or any service credits, and i2i shall not be in default under any agreement for i2i Services, if its compliance with any Investigation causes a User to incur downtime or requires the sequestering of all or a portion of the Servers. i2i also reserves the right to disclose information relating to Users and their use of i2i Services, i2i Network or its physical infrastructure or information transmitted, owned by or stored by or on behalf of any User, if such information is disclosed in connection with an Investigation or in order to prevent the death of or bodily harm to any individual, as determined by i2i in its sole discretion.**

13) Violations of AUP - i2i may enforce the i2i AUP, with or without notice to a User, by any action it deems reasonable, in its sole discretion. In addition to the remedial provisions provided elsewhere in the i2i AUP, i2i may:
a) Disable access to a User's content that violates the i2i AUP;
b) Suspend or Terminate a User's access to i2i Services, i2i Network or its physical infrastructure;
c) Remove DNS records from Servers;
d) Block mail or any other network service;
e) Effect IP address null routing;
f) Take legal action against a User to enforce compliance with the i2i AUP;

Acceptable Use Policy

i2i will not be held responsible for loss of productivity, revenue, or any perceived or real loss of any kind resulting from the termination of Customer services due to violations of the i2i AUP.

14) **Reporting Violations - If you believe that a violation of the i2i AUP has occurred please review the information in the Resource section at www.trusti2i.com which contains important information concerning the reporting of potential violations.** Direct all suspected violations of the i2i AUP and supporting information to the Abuse Department at abuse@trusti2i.com. If available, please provide the following information:
    a) The IP address used to commit the alleged violation;
    b) The date and time of the alleged violation, including the time zone or offset from CST;
    c) Evidence of the alleged violation.
    d) E-mail with full header information provides all of the above, as do system log files. Other situations will require different methods of providing the above information. i2i may take any one or more of the following actions in response to complaints:
        i) Issue written or verbal warnings;
        ii) Suspend the User's newsgroup posting privileges;
        iii) Suspend the User's account;
        iv) Terminate the User's account;
        v) Bill the User for administrative costs and/or reactivation charges;
        vi) Bring legal action to enjoin violations and/or to collect damages, if any, cause by violations

If any User uses i2i's Website, Facilities, Network Environment, Computing Environment, and Services (collectively, "Services" and each a "Service") in a manner that exposes i2i to potential liability, as reasonably determined by i2i, i2i may suspend permanently or terminate the users access.

The remedial actions set forth in the i2i AUP shall not be construed in any way to limit the actions or remedies that i2i may take to enforce and ensure compliance with the i2i AUP. i2i reserves the right to recover any and all expenses, and apply any reasonable charges, in connection with a User's violation of the i2i AUP. No refund or service credits will be issued for any interruption in service resulting from violations of the i2i AUP.

i2i reserves the right at all times to investigate any actual, suspected, or alleged violations of the i2i AUP, with such investigation to include accessing of data and records on, or associated with, any Server, i2i Network or its physical infrastructure.