NetSource Acceptable Use Guidelines

1. Use of Services

1.1. The Customer agrees to use NetSource's services only for lawful purposes, in compliance with all applicable laws. Specific activities that are prohibited include, but are not limited to:

- Threatening harm to persons or property or otherwise harassing behavior.
- Violating U.S. export control laws for software or technical information.
- Fraudulently representing products/services using your account.
- Initiating a Denial of Service (DOS) attack in any form.
- Sending SPAM.
- Facilitating, aiding, or encouraging any of the above activities.

Additional activities are prohibited that appear in further sections of these guidelines, including section 2.0 Use of Material and 3.0 System Security.

1.2. The customer agrees not to publish pornography on any server or account hosted at NetSource.

1.3. NetSource reserves the right to investigate suspected violations of these Guidelines. When NetSource becomes aware of possible violations, NetSource may initiate an investigation which may include gathering information from the Customer or Customers involved and the complaining party.

During an investigation, NetSource may block access at the router level to customer's equipment involved. If NetSource believes, in its sole discretion, that a violation of these Guidelines has occurred, it may take responsive action. Such action may include, but is not limited to, temporary or permanent blocking of access to customer's equipment, and the suspension or termination of the customer's service.

NetSource, in its sole discretion, will determine what action will be taken in response to a violation on a case-by-case basis. Violations of these Guidelines could also subject the Customer to criminal or civil liability.

1.4. The Customer of record is responsible for all use of the services and co-location space, with or without the knowledge or consent of the Customer.

2. Use of Material

2.1. Materials in the public domain (e.g., images, text, and programs) may be downloaded or uploaded using NetSource services. Customers may also re-distribute materials in the public domain.

The Customer assumes all risks regarding the determination of whether the material is in the public domain.

2.2. The Customer is prohibited from storing, distributing or transmitting any unlawful material through NetSource services. Examples of unlawful material include but are not limited to direct

threats of physical harm, child pornography, and copyrighted, trademarked and other proprietary material used without proper authorization. The Customer may not post, upload or otherwise distribute copyrighted material on NetSource's servers without the consent of the copyright holder. The storage, distribution, or transmission of unlawful materials could subject the Customer to criminal as well as civil liability, in addition to the actions outlined in 1.3 above.

2.3. The Customer may not store or distribute certain other types of material. Examples of prohibited material include, but are not limited to, programs containing viruses or Trojan horses and tools to compromise the security of other sites, tools used to collect email addresses for use in sending bulk email, or tools used to send bulk mail.

2.4. Each NetSource Customer is responsible for the equipment security of his or her password. Generally, secure passwords are between 6 and 8 characters long, contain letters of mixed case and non-letter characters, and cannot be found in whole or in part, in normal or reverse order, in any dictionary of words or names in any language. The Customer is responsible for changing his or her equipment or service password regularly.

2.5. NetSource staff may monitor the security of Customer passwords at any time. A Customer with an insecure password may be directed to change the password to one which complies with the above rules. Customers who repeatedly choose insecure passwords may be assigned a password by NetSource.

2.6. NetSource Customers are provided a Door Access Code and a KeyFOB or Key Card for each Customer Representative that may enter the data center unattended. Customer Representatives agree to guard their Door Access Codes, KeyFOBs, and Key Cards and not share them with other people. All such Customer Representatives also agree to read, understand, sign, and comply with the NetSource Data Center Policies document for their safety and the security of the data center.

3. System Security

3.1. The Customer is prohibited from utilizing NetSource services to compromise the security or tamper with system resources or accounts on computers at NetSource or at any other site. Use or distribution of tools designed for compromising security is prohibited. Examples of these tools include but are not limited to password guessing programs, cracking tools or network probing tools.

3.2. NetSource reserves the right to release the contact information of Customers involved in violations of system security to system administrators at other sites, in order to assist them in resolving security incidents. NetSource will also fully cooperate with law enforcement authorities in investigating suspected lawbreakers.

4. Email Use

4.1. NetSource will investigate complaints regarding email and may, in its sole discretion, take action based on the rules below. If an email message is found to violate one of the policies below, or to contain unlawful material, as described in 2.2 and 2.3 above, NetSource may take action as outlined in 1.3 above.

4.2. NetSource Customers may not send email in any way that may be illegal. NetSource recognizes that email is an informal medium; however, Customers must refrain from sending further email to a user after receiving a request to stop.

4.3. Unsolicited advertising mailings, whether commercial or informational, are strictly prohibited. NetSource Customers may send advertising material only to addresses which have specifically requested that material.

4.4. NetSource Customers may not send, propagate, or reply to mail bombs. Mail bombing is defined as either emailing copies of a single message to many Customers, or sending large or multiple files or messages to a single user with malicious intent.

4.5. NetSource Customers may not alter the headers of email messages to conceal their email address or to prevent Customers from responding to messages.

4.6. Violations of the NetSource policies outlined in this document can sometimes result in massive numbers of email responses. If an NetSource Customer receives so much email that NetSource resources are affected, NetSource staff may block access to the customer's equipment at the router level.

5. World Wide Web Use

5.1. NetSource will investigate complaints regarding inappropriate material on Web pages transmitted using NetSource services, in its sole discretion, require that the material be removed or take action as outlined in 1.3 above.

If you do not agree to be bound by these Acceptable Use Guidelines, please notify NetSource Customer Service, support@ntso.com so that we may initiate a closure of your account.