Acceptable Use Policy

This Acceptable Use Policy ("AUP") sets forth the acceptable use of EXIGO networks, Services, and On-Demand Services. All users of EXIGO networks, Services, and On-Demand Services must comply with this policy and all applicable laws and regulations, in addition to all terms and conditions of applicable agreements, and any additional policies that may be applicable to a specific service offered by EXIGO. EXIGO strives to provide the highest quality Internet services available, while at the same time respecting the standards that have been created both within the Internet community and by legislation. Inappropriate or abusive activities and conduct will not be tolerated on EXIGO networks. EXIGO reserves the right to modify this AUP from time to time, without notice. Users of EXIGO networks are encouraged to review this AUP often for changes or new information. Please send questions, comments, or complaints regarding this AUP to mailto: abuse@EXIGO.com This Agreement was last updated on February 25, 2016.

COMPLIANCE

Duties

Each user is responsible for complying with this AUP, and for providing assistance to EXIGO in investigating and resolving any issue, as EXIGO may request from time to time. Additionally, You and Your users are required to determine the conditions of, and comply with, the acceptable use policies or equivalent documents of all network(s) which Your data transits.

Users will be held responsible for the actions of any third party agent that acts on their behalf or for their benefit and shall be held directly accountable for any violations of this AUP by third party agents.

EXIGO does not control the content of data traversing EXIGO networks; accordingly, EXIGO assumes no responsibility for the content of any data or communication that may be transmitted over EXIGO networks.

Configuration

- All systems which are connected to EXIGO networks shall be configured in accordance with industry standards, applicable laws and regulations.
- Systems connected to EXIGO networks shall not be configured in any way which obscures system-identity information.
- Proxy servers of any kind shall be configured so as to prevent unauthenticated use from the public Internet.

Reporting Obligations

Users of EXIGO are responsible for immediately reporting to EXIGO any issues, which could

compromise the stability, service or security of any user or system connected to EXIGO networks.

Resellers and Downstream Service Providers

Resellers of EXIGO services are responsible for informing their customers of this AUP and for enforcing its restrictions with regard to their customers' actions. Breach or non-compliance of this AUP by a reseller's customer or end-user shall be considered a violation by the reseller and the customer or end-user of this AUP.

PROHIBITED USES

These lists are not meant to be exhaustive, but merely illustrative of examples of inappropriate and improper conduct, which are prohibited on EXIGO networks.

Illegal Use

EXIGO's Networks may only be used for lawful purposes. The transmission, distribution, or storage of any data or material in violation of any applicable law or regulation is prohibited. This includes, but is not limited to material or data which:

- Infringes any copyright, trademark, trade secret, or other intellectual property right.
- Violates export control laws or regulations.
- Violates any party's confidentiality rights.
- Constitutes use or dissemination of child pornography.
- Is illegal or unlawful.

Abuse

The following general actions are considered "abuse" and are strictly prohibited:

- Any conduct which is inconsistent with generally accepted norms and expectations of the Internet community (whether or not detailed in this AUP). EXIGO reserves the right, in its sole discretion, to make a determination of whether any particular conduct violates such norms and expectations.
- Using EXIGO networks to transmit material that EXIGO believes to be illegal.
- Forging of message headers or identity information, or taking any action with the intent of bypassing restrictions or limits on access to a specific service or site. This prohibition does not restrict the legitimate non-commercial use of pseudonymous or anonymous services.

Security

Users of EXIGO networks must configure their systems in a secure manner. Should a user's system be exploited by unauthorized persons, the user is responsible for both reporting the violation (where applicable), and then fixing the exploited system. For instance, should the security of a mail server be compromised to distribute unsolicited emails, the user is responsible for immediately re-configuring the system to prevent further unauthorized use.

Users are prohibited from interfering or attempting to interfere with services ("Denial of Service Attacks"), whether intentionally or through neglect, of any other user, host, or network. The prevention of "unintentional attacks", such as infection and subsequent propagation of computer viruses, are the responsibility of every user.

E-Mail

Users are prohibited from engaging in improper use or distribution of electronic mail ("e-mail"). Users are strictly prohibited from engaging in any of the following activities:

- Sending unsolicited mass or commercial e-mail ("spamming") for any purpose whatsoever.
- Having third parties send out commercial emails on any user's behalf. Using EXIGO facilities to receive replies from unsolicited emails (commonly referred to as "drop-box" accounts).
- Configuring any email server in such a way that it will accept third party emails for forwarding (commonly known as an "open mail relay"). If a site has roaming users who wish to use a common mail server, the mail server must be configured to require some form of user identification and authorization.

Mass or commercial email may be sent only to recipients who have expressly requested receipt of such e-mails, by the sending of an email request to the person performing the mass or commercial mailings. This exchanging of requests, acknowledgements, and final confirmations (commonly referred to as a "double opt-in" process) must be adhered to in its entirety for any mass or commercial email to be considered "solicited" by EXIGO.

Users that send mass or commercial e-mail are required to maintain complete and accurate records of all e-mail subscription requests, specifically including the email and associated headers sent by every e-mail subscriber, and to immediately provide EXIGO with such records upon request of EXIGO. E-mail subscriptions that do not have a specific recipient generated email request associated with them are invalid, and are strictly prohibited.

Exigo will allow the passing of email opt-in information as long as the subscribedate and subscribeIP information that is passed is verifiable. Exigo will randomly check this information and confirm the source. There can not be any subscribeIP in the Exigo database that is used more than 3 times.

In the absence of positive, verifiable proof to the contrary, EXIGO considers complaints by recipients of e-mails to be de-facto proof that the recipient did not subscribe or otherwise request the e-mail(s) about which a complaint was generated.

Enforcement

EXIGO will provide notice to You of violation(s) of any provisions of this policy with written notice, which notice can be provided via e-mail, fax or USPS, with the desire that You cure the violation(s). Prior to suspension or termination, EXIGO will attempt to work with You to cure violations of this policy and ensure that there is no re-occurrence; however, EXIGO reserves the right to suspend or terminate based on a first offense, after attempting to resolve the violation with 3rd party providers as required by backbone providers, SPAM regulatory services, or as required by State or Federal Law.