AUBURN ESSENTIAL SERVICES
ACCEPTABLE USE POLICY

This Acceptable Use Policy (AUP) sets forth guidelines for acceptable use of the Auburn Broadband Network (“ABN”). All users of the ABN are required to comply with this policy. Users must also comply with all terms and conditions of applicable agreements, and with any additional policies that may be applicable to a specific service offered by the City of Auburn, Indiana through its Essential Services Division (“AES”).

By using AES’ services, you agree to abide by, and require others using the services via your account to abide by the terms of this AUP. You should consult this document regularly to ensure that your activities conform to the most recent version. **IF YOU DO NOT AGREE TO BE BOUND BY THESE TERMS, YOU SHOULD IMMEDIATELY STOP THE USE OF AES SERVICES AND NOTIFY THE AES CUSTOMER SERVICE DEPARTMENT SO THAT YOUR ACCOUNT MAY BE CLOSED.**

Compliance Responsibilities

AES provides an unfiltered connection to the Internet and voice services based upon Internet Protocol (IP). No data, documents, materials, or information that enters the ABN is reviewed before being transmitted to users. Accordingly, AES neither controls nor accepts responsibility for the content of any communications that are transmitted or made available to users, regardless of whether they originated from users of the ABN. In addition, AES expressly disclaims any responsibility for the accuracy or quality of information provided by third parties that may be obtained through the use of the ABN. Each user is responsible for complying with this Acceptable Use Policy, and for providing reasonable assistance to AES in investigating and resolving issues, problems, and/or complaints arising out of the services provided to such user.

Conformance With Policies of Other ISPs

In situations where data communications are carried across networks of other Internet Service Providers (ISPs), users of the ABN must also conform to the applicable acceptable use policies of such other ISPs.

Configuration

All users of the ABN are responsible for configuring their own systems to provide the maximum possible accountability. For example, users should ensure there are clear "path" lines in news headers so that the originator of a post may be identified. Users should also configure their Mail Transport Agents (MTA) to authenticate (by look-up on the name or similar procedures) any system that connects to perform a mail exchange, and should generally present header data as clearly as possible. As another example, users should maintain logs of dynamically assigned IP addresses.

Consequences of Non-Compliance

Violation of this Acceptable Use Policy is strictly prohibited. In the event of any actual or potential violation, AES reserves the right to suspend or terminate, either temporarily or permanently, any or all services provided by Auburn, to block any abusive activity, or to take any other actions as deemed appropriate by AES in its sole discretion. Users who violate this Acceptance Use Policy may incur criminal or civil liability. AES may refer violators to civil or criminal authorities for prosecution, and will cooperate fully with applicable government authorities in connection with the civil or criminal investigations of violations.

Prohibited Use

The examples of prohibited use set forth below and throughout this Acceptable Use Policy are non-exclusive, and are provided as guidelines to customers and other users of the ABN.

Illegal Use

The ABN may be used only for lawful purposes. The transmission, distribution, or storage of any information, data, or material in violation of any applicable law or regulation is prohibited. Without limitation of the foregoing, it is strictly prohibited to create, transmit, distribute, or store any information, data, or material which:

- Infringes any copyright, trademark, trade secret, or other intellectual property right.
- Is obscene or constitutes child pornography.
- Is libelous, defamatory, hateful, or constitutes an illegal threat or abuse.
- Violates export control laws or regulations.
- Encourages conduct that would constitute a criminal offense or give rise to civil liability.
- Deceptive on-line marketing practices.

In the event of suspected, alleged, or actual illegal activity, AES will notify or cooperate with applicable law enforcement authorities for potential civil or criminal investigation or prosecution.

Abuse

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

- Any conduct which violates the accepted norms and expectations of the Internet community at large (whether or not detailed in this Acceptable Use Policy). AES reserves the right, in its sole discretion, to make a determination whether any particular conduct violates such norms and expectations.
- Resale of AES' services or products, unless expressly authorized in a separate written agreement with AES.
- Any conduct that restricts or inhibits any other user, whether a customer of AES or a user of any other system or network, from using or enjoying any of AES' services or products, as determined by AES in its sole discretion.
- Harassment, whether through language, frequency, or size of messages.
- Creating, forwarding, posting, or distribution of chain messages of any type (also known as "pyramid" or "Ponzi" schemes).
- Forging of message headers or a sender's identity, or taking any similar action with the intent of bypassing restrictions or limits on access to a specific service or site (such as a moderated newsgroup or a site utilizing filters). This prohibition does not restrict the legitimate use of aliases or anonymous re-mailers.
- Falsifying identity or contact information (whether given to AES, to the InterNIC, or put in a message header) to circumvent this Acceptable Use Policy. This prohibition does not restrict the legitimate use of aliases or anonymous re-mailers.

- Furnishing false or incorrect data to AES on written or online applications, contracts, or other materials or information provided to AES, including fraudulent use of credit card numbers or "bill to" telephone numbers.
- Effecting or attempting security breaches or disruptions of Internet communications. Security breaches include, but are not limited to, accessing data of which customer is not an intended recipient or logging onto a server or account that customer is not expressly authorized to access. For purposes of this section, "disruption" refers to the incidents/conditions as understood by the Internet community at large and includes, but is not limited to, port scans, ping floods, packet spoofing, forged routing information, deliberate attempts to overload a service, and attempts to "crash" a host.
- Attempting to circumvent or alter the processes or procedures to measure time, bandwidth utilization, or other methods to document use of AES' products and services.
- Attempting to circumvent user authentication or security of any host, network, or account ("cracking"). This includes, but is not limited to, accessing data not intended for the customer, logging into a server or account the customer is not expressly authorized to access, or probing the security of other networks.
- Executing any form of network monitoring which will intercept data not intended for Customer.

Security
Violations of system or network security are prohibited, and may result in criminal and civil liability. AES will investigate potential security violations, and may notify applicable law enforcement agencies if violations are suspected.

It is strictly prohibited to attempt to circumvent the authentication procedures or security of any host, network, network component, or account (i.e. "cracking") to access data, accounts, or servers that the user is not expressly permitted or authorized to access. This prohibition applies whether or not the attempted intrusion is successful, and includes unauthorized probes or scans performed with the intent to gather information on possible security weaknesses or exploitable configurations.

Users of the ABN are responsible for educating themselves and configuring their systems with at least basic security as generally accepted by the Internet community at large. Should systems at a user's site be violated, the user is responsible for reporting the violation and then fixing the exploited system. For instance, should a site be abused to distribute unlicensed software due to a poorly configured FTP (File Transfer Protocol) Server, the user is responsible for re-configuring the system to stop the abuse.

Users are prohibited from interfering or attempting to interfere with service to any other user, host, or network on the Internet ("denial of service attacks"). Examples of such prohibited activity include without limitation (a) sending massive quantities of data (i.e. "ping flooding" with ICMP, SMTP, or any other type of traffic that exceeds accepted norms of size and/or frequency) with the intent of filling circuits, overloading systems, and/or crashing hosts, (b) attempting to attack or disable any user, host, or site, or (c) using, distributing, or propagating any type of program, script, or command designed to interfere with the use, functionality, or connectivity of any Internet user, host, system, or site (for example, by propagating messages, via e-mail, Usenet posting , or otherwise, that contain computer worms, viruses, control characters or Trojan horses).

Users are prohibited from intentionally or negligently injecting false data into the Internet, for instance in the form of bad routing information (including but not limited to the announcing of networks owned by someone else or reserved by the Internet Assigned Numbers Authority) or incorrect DNS information.

E-Mail
Users are prohibited from engaging in improper use or distribution of electronic mail ("e-mail") over the Internet. Without limitation of the foregoing, it is strictly prohibited to engage in any of the following activities:

- Sending unsolicited bulk e-mail ("UBE", or "spamming"). This includes, but is not limited to, the distribution of UBE for commercial, informational, advertising, political, or religious purposes.
- Using a mail transport agent (MTA) outside of a user's own site to relay mail (unless a user has received express permission to do so). Even if permission has been received, users are prohibited from forging their identities to make it appear as though the e-mail sourced from the relay.
- Willful failure to secure open SMTP ports so as to prevent the unauthorized use of customer resources for the purposes of sending unsolicited e-mail by a third party.

Bulk e-mail may be sent only to recipients who have expressly requested receipt of such e-mail. Users that send solicited bulk e-mail are required to maintain records of all bulk e-mail subscription requests, and to provide AES with such records upon request of AES, to enable AES to investigate complaints from third parties. The sender of any solicited bulk e-mail shall, upon the request of a recipient, immediately remove such recipient from all applicable mailing lists and refrain from further transmissions of e-mail to such recipient.

USENET (also known as NETNEWS or NEWSGROUPS)
Without limitation, it is strictly prohibited to engage in any of the following activities:

- Making any posting for commercial purposes (including without limitation the pointing to specific URLs for commercial purposes), except where such postings are expressly permitted under the charter and/or Frequently Asked Questions (FAQ) of an applicable newsgroup.
- Posting binary files to newsgroups whose charter or name does not include allowances for such files.
- Canceling newsgroup postings other than their own, or using auto-responders or cancel-bots (or similar automated or manual routines) that generate excessive

network traffic or disrupt Usenet newsgroup/e-mail use by others (except in cases of official newsgroup moderators performing their duties).

- Engaging in "Excessive Cross-Posting" (ECP) or "Excessive Multi-Posting" (EMP) or "Usenet spam" (no matter what the content might be) as defined by the Internet community.
- Disrupting newsgroups with materials, postings, or activities that are (as determined by AES in its sole discretion) frivolous, unlawful, obscene, threatening, abusive, libelous, hateful, excessive, or repetitious, unless such materials or activities are expressly allowed or encouraged under the newsgroup's name, FAQ, or charter.
- Failure to secure a news server, so as to prevent the unauthorized use of customer resources by a third party, which may result in Usenet posts that violate this policy.
- Performing any unauthorized creation, cancellation, or removal of newsgroups.

World Wide Web
AES strictly prohibits users from engaging in any of the following web-related activities:

- The exploitation or attempted exploitation of any scripts presented on web pages (e.g. forms for answering questions or for entering data).
- Excessive use of bandwidth by utilizing programs, scripts, or commands to abuse a web site (for example, by connecting for an excessive amount of time, repeatedly engaging site-local scripts, or related behavior).
- "Walking" a database for the purpose of collecting data contained therein (whether or not this behavior requires that the reader of the page must knowingly ignore files such as "robot.txt" which is designed to guide cataloguing robots/programs).
- Operating a robot on a site's page after the site has asked that the behavior cease.
- Configuring a web page to act maliciously against users that visit that web page.

Filing Complaints and Contact Information for AES Customers
Any complaints regarding prohibited use or other abuse of the ABN, including violations of this Acceptable Use Policy, should be sent via e-mail to AES at: Connect@ci.auburn.in.us. Please include all applicable information that will assist AES in investigating the complaint, including all applicable header lines of forwarded messages. If you are unsure whether any contemplated use or action is permitted, please send questions or comments to AES at: Connect@ci.auburn.in.us. For further information about this Acceptable Use Policy, please contact AES at:

PO Box 506 / 210 S Cedar St, 2nd Floor City Hall
Auburn, IN 46706
260.333.0100