Acceptable Use Policy

As providers of communications services, Bluebird Network, LLC and its affiliates (collectively, "Bluebird") offer their customers and users the means to acquire and disseminate information utilizing the Internet. Because of the nature of the Internet, Bluebird reserves the right to take certain preventative or corrective actions to protect its network, its customers, and users, which are outlined in this Acceptable Use Policy ("Policy"). This Policy, including the following list of Prohibited Activities, outlines certain terms to which Bluebird's customers and their users are expected to adhere and is intended as a guide to the obligations of customers and their users when using Bluebird's services. Bluebird may revise this Policy from time to time.

Prohibited Uses of Bluebird Systems and Services:

1. Transmission, distribution or storage of any material in violation of any applicable law or regulation. This includes, without limitation, any material that infringes or misappropriates the intellectual property of others, including copyrights, trademarks, service marks, trade secrets, or other intellectual property used without proper authorization, and material that is obscene, defamatory, abusive, harassing, threatening, or violates export control laws.
2. The sending of any form of Unsolicited Bulk Email ("UBE" or "spam"), Internet viruses, worms, Trojan horses, pinging, flooding, mail-bombing, or denial of service attacks utilizing Bluebird's network. Likewise, the sending of these materials from another service provider advertising a web site, email address or utilizing any resource hosted on Bluebird's servers, is prohibited. Bluebird accounts or services may not be used to solicit customers from, or collect replies to, messages sent from another Internet Service Provider where those messages violate this Policy.
3. Subscribing email addresses to any mailing list without the consent of the email address owner.
4. Forging or misrepresenting message headers, whether in whole or in part, to mask the originator of the message.
5. Advertising, transmitting, or otherwise making available any software, program, product, or service that violates this Policy, which includes, but is not limited to, the facilitation of the means to send Unsolicited Bulk Email, Internet viruses, worms, Trojan horses, pinging, flooding, mail-bombing, or denial of service attacks.
6. Operating an account on behalf of, or in connection with, or reselling any service to, persons or firms listed in the Spamhaus Register of Known Spam Operations (ROKSO) database at www.spamhaus.org.
7. Accessing illegally, or without authorization, computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system. This includes any activity that might be used as a precursor to such conduct, including a port scan, stealth scan, or other information gathering activity.
8. Obtaining or attempting to obtain service by any means or device with intent to avoid payment.
9. Using Bluebird's services to interfere with the use of the Bluebird network by other customers or authorized users.
10. Engaging in any activity that is determined to be illegal, including advertising, transmitting, or otherwise making available Ponzi schemes, pyramid schemes, fraudulently charging credit cards, and pirating software.

Customer Responsibility for Customer's Users

Each Bluebird customer is responsible for the activities of its users, and, by accepting service from Bluebird, customer agrees that its users are subject to and will abide by this Policy. If a customer or its user violates this Policy, Bluebird reserves the right to terminate the customer's service or take action to stop the customer or its user from violating this Policy as Bluebird deems appropriate, without notice.

Bluebird may temporarily suspend traffic to and from a customer's IP address in the event of a (a) denial of service attack, (b) botnet, (c) propagation of computer viruses or other programs, (d) malicious and premeditated congestion of Bluebird's network, (e) falsification of the identity of packages and messages (including modification of the heading of TCP/IP packages, electronic mail messages and message), or (f) other similar attacks on Bluebird's network or customers, in each case originating from or directed towards an IP address of customer or its user and posing a threat of material harm to Bluebird's network or customers.

Last updated: 10/09/2013