Highland Networks, LLC (Seller) is committed to complying with the laws and regulations governing use of the Internet, e-mail transmission and text messaging; and preserving for all of its Customers the ability to use Seller's network and the Internet without interference or harassment from other users. The **Highland Networks, LLC** Acceptable Use Policy ("AUP") is designed to help achieve these goals.

By using certain Internet Protocol based Services (the "IP Services"), as defined below, the Customer agrees to comply with this Acceptable Use Policy and to remain responsible for all of its users. Seller reserves the right to change or modify the terms of this AUP at any time. Seller will provide Customer with a copy of the current AUP at any time upon receipt of Customer's request.

1.1 Scope of AUP

The AUP applies to the Seller services that provide (or include) access to the Internet, including hosting services (software applications and hardware), or are provided over the Internet or wireless data networks (collectively "IP Services").

1.2 Prohibited Activities

General Prohibitions: Seller prohibits use of the IP Services in any way that is unlawful, harmful to or interferes with use of Seller's network or systems, or the network of any other provider, interferes with the use or enjoyment of services received by others, infringes intellectual property rights, results in the publication of threatening or offensive material, or constitutes Spam/E-mail/Usenet abuse, a security risk or a violation of privacy.

Failure to adhere to the rules, guidelines or agreements applicable to search engines, subscription web services, chat areas, bulletin boards, web pages, applications, or other services that are accessed via a link from a Seller-branded website or from a website that contains Seller-branded content is a violation of this AUP.

Unacceptable Behavior: The following is deemed unacceptable use or behavior by employees of companies utilizing Seller IP Services:

- visiting Internet sites that contain obscene, hateful, pornographic or otherwise illegal material,
- using the computer to perpetrate any form of fraud, or software, film or music piracy,
- using the Internet to send offensive or harassing material to other users,
- downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such license,
- hacking into unauthorized areas,
- publishing defamatory and/or knowingly false material about a business entity, your colleagues and/or our customers on social networking sites, blogs, online journals, wikis or any online publishing format,

- revealing confidential information about a business entity in a personal online posting, upload or transmission including financial information and information relating to our customers, business plans, policies, staff and/or internal discussions,
- undertaking deliberate activities that waste staff effort or networked resources, OR
- introducing any form of malicious software into the Seller network.

Threatening Material or Content: IP Services shall not be used to host, post, transmit, or re-transmit any content or material (or to create a domain name or operate from a domain name), that harasses, or threatens the health or safety of others. In addition, for those IP Services that utilize Seller provided web hosting, Seller reserves the right to decline to provide such services if the content is determined by Seller to be obscene, indecent, hateful, malicious, racist, defamatory, fraudulent, libelous, treasonous, excessively violent or promoting the use of violence or otherwise harmful to others.

Unlawful Activities: IP Services shall not be used in connection with any criminal, civil or administrative violation of any applicable local, state, federal, national or international law, treaty, court order, ordinance, regulation or administrative rule.

Violation of Intellectual Property Rights: IP Services shall not be used to publish, submit/receive upload/download, post, use, copy or otherwise reproduce, transmit, re- transmit, distribute or store any content/material or to engage in any activity that infringes, misappropriates or otherwise violates the intellectual property rights or privacy or publicity rights of Seller or any individual, group or entity, including but not limited to any rights protected by any copyright, patent, trademark laws, trade secret, trade dress, right of privacy, right of publicity, moral rights or other intellectual property right now known or later recognized by statute, judicial decision or regulation.

Inappropriate Interaction with Minors: Seller complies with all applicable laws pertaining to the protection of minors, including when appropriate, reporting cases of child exploitation to the National Center for Missing and Exploited Children.

Child Pornography: IP Services shall not be used to publish, submit/receive, upload/download, post, use, copy or otherwise produce, transmit, distribute or store child pornography. Suspected violations of this prohibition may be reported to Seller through its customer service contact number. Seller will report any discovered violation of this prohibition to the National Center for Missing and Exploited Children and take all steps necessary to remove child pornography (or otherwise block access to the content determined to contain child pornography) from its servers.

Spam/E-mail/Usenet Abuse: Violation of applicable laws regulating e-mail services, constitute a violation of this AUP. Any abuse that results in a blacklist will result in a $10 per blacklist fee to perform cleaning.

Spam/E-mail or Usenet abuse is prohibited using IP Services. Examples of Spam/E-mail or Usenet abuse include but are not limited to the following activities:

- sending multiple unsolicited electronic mail messages or “mail-bombing” – to one or more recipient;

- sending unsolicited commercial e-mail, or unsolicited electronic messages directed primarily at the advertising or promotion of products or services;
- sending unsolicited electronic messages with petitions for signatures or requests for charitable donations;
- sending bulk electronic messages without identifying, within the message, a reasonable means of opting out from receiving additional messages from the sender;
- sending electronic messages, files or other transmissions that exceed contracted for capacity or that create the potential for disruption of the Seller network or of the networks with which Seller interconnects, by virtue of quantity or size;
- using another site's mail server to relay mail without the express permission of that site;
- using another computer, without authorization, to send multiple e-mail messages or to retransmit e-mail messages for the purpose of misleading recipients as to the origin or to conduct any of the activities prohibited by this AUP;
- using IP addresses that the Customer does not have a right to use;
- collecting the responses from unsolicited electronic messages;
- maintaining a site that is advertised via unsolicited electronic messages, regardless of the origin of the unsolicited electronic messages;
- sending messages that are harassing or malicious, or otherwise could reasonably be predicted to interfere with another party's quiet enjoyment of the IP Services or the Internet (e.g., through language, frequency, or size;
- using distribution lists containing addresses that include those who have opted out;
- sending electronic messages that do not accurately identify the sender, the sender's return address, the e-mail address of origin, or other information contained in the subject line or header;
- falsifying packet header, sender, or user information whether in whole or in part to mask the identity of the sender, originator or point of origin;
- posting a message to more than ten (10) online forums or newsgroups, that could reasonably be expected to generate complaints;
- intercepting, redirecting or otherwise interfering or attempting to interfere with e-mail intended for third parties;
- knowingly deleting any author attributions, legal notices or proprietary designations or labels in a file that the user mails or sends;
- using, distributing, advertising, transmitting, or otherwise making available any software program, product, or service that is designed to violate this AUP or the AUP of any other Internet Service Provider, including, but not limited to, the facilitation of the means to spam.

Spam Handling

The seller handles spam on a three strike system. The customer will not hold the seller liable for actions taken under the three strike system. Three strikes may result in termination of services and closure of client account. Customer forfeits all rights to systems after third strike is reached.

1.3 Security Violations

Customers are responsible for ensuring and maintaining security of their systems and the machines that connect to and use IP Services, including implementation of necessary patches and operating system updates.

IP Services may not be used to interfere with, gain unauthorized access to, or otherwise violate the security of Seller's (or another party's) server, network, network access, personal computer or control devices, software or data, or other system, or to attempt to do any of the foregoing.

Examples of system or network security violations include but are not limited to:

- unauthorized monitoring, scanning or probing of network or system or any other action aimed at the unauthorized interception of data or harvesting of e-mail addresses;
- hacking, attacking, gaining access to, breaching, circumventing or testing the vulnerability of the user authentication or security of any host, network, server, personal computer, network access and control devices, software or data without express authorization of the owner of the system or network; • impersonating others or secretly or deceptively obtaining personal information of third parties (phishing, etc.);
- using any program, file, script, command or transmission of any message or content of any kind, designed to interfere with a terminal session, the access to or use of the Internet or any other means of communication;
- distributing or using tools designed to compromise security (including but not limited to SNMP tools), including cracking tools, password guessing programs, packet sniffers or network probing tools (except in the case of authorized legitimate network security operations);
- knowingly uploading or distributing files that contain viruses, spyware, Trojan horses, worms, time bombs, cancel bots, corrupted files, root kits or any other similar software or programs that may damage the operation of another's computer, network system or other property, or be used to engage in modem or system hi-jacking;
- engaging in the transmission of pirated software;
- with respect to dial-up accounts, using any software or device designed to defeat system time-out limits or to allow Customer's account to stay logged on while Customer is not actively using the IP Services or using such account for the purpose of operating a server of any type;
- using manual or automated means to avoid any use limitations placed on the IP Services;
- providing guidance, information or assistance with respect to causing damage or security breach to Seller's network or systems, or to the network of any other IP Service provider;
- failure to take reasonable security precautions to help prevent violation(s) of this AUP.

1.4 AUP Monitoring and Enforcement

Customer's failure to observe the guidelines set forth in this AUP may result in Seller taking actions anywhere from a warning to a suspension or termination of Customer's IP Services.

When feasible, Seller may provide Customer with a notice of an AUP violation via e-mail or otherwise allowing the Customer to promptly correct such violation.

Seller reserves the right to act immediately and without notice to suspend or terminate affected IP Services in response to a court order or government notice that certain conduct must be stopped or when Seller reasonably determines, that the conduct may: (1) expose Seller to sanctions, prosecution, civil action or any other liability, (2) cause harm to or interfere with the integrity or normal operations of Seller's network or networks with which Seller is interconnected, (3) interfere with another Seller Customer's use of IP Services or the Internet (4) violate any applicable law, rule or regulation, or (5) otherwise present an imminent risk of harm to Seller or Seller Customers.

Seller may also terminate a Customer pursuant to its policy of terminating in appropriate circumstances users and customers whom Seller determines, in its sole discretion, are repeat infringers as contemplated by the Digital Millennium Copyright Act.

Seller has no obligation to monitor content of any materials distributed or accessed using the IP Services. However, Seller may monitor content of any such materials as necessary to comply with applicable laws, regulations or other governmental or judicial requests; or to protect the Seller network and its customers.

1.5 Customer Responsibilities

Customers remain solely and fully responsible for the content of any material posted, hosted, downloaded/uploaded, created, accessed or transmitted using the IP Services. Seller has no responsibility for any material created on the Seller's network or accessible using IP Services, including content provided on third-party websites linked to the Seller network. Such third- party website links are provided as Internet navigation tools for informational purposes only, and do not constitute in any way an endorsement by Seller of the content(s) of such sites.

Customers are responsible for taking prompt corrective action(s) to remedy a violation of AUP and to help prevent similar future violations. Use of the Internet by employees of the Customer is permitted and encouraged where such use supports the goals and objectives of the business. However, it is expected that the Customer will have a policy for the use of the Internet whereby Customer and its employees shall:

- Comply with current legislation governing Acceptable Use,
- Use the Internet in an acceptable way,
- Not create unnecessary business risk to the company by their misuse of the Internet,
- Have an Internet Acceptable Use Policy in place and distributed to all employees, AND
- Resolve any situations with an employee where the Internet Acceptable Use Policy has been violated.

If any Internet use issues by the Customer account are discovered by Seller personnel while monitoring and maintaining IP Service, Seller will relay that information to the Customer.

1.6 Incident Reporting

Any complaints (other than claims of copyright infringement) regarding violation of this AUP by a Seller Customer (or its user) should be directed to Seller at the contact information below. Where possible, include details that would assist Seller in investigating and resolving such complaint (e.g. expanded headers, IP address(s), a copy of the offending transmission and any log files).

Contact Information: Any notification that Seller sends to its Customers pursuant to this AUP will be sent via e-mail to the e-mail address on file with Seller, or may be in writing to Customer's address of record. It is Customer's responsibility to promptly notify Seller of any change of contact information.

1.7 DMCA Compliance

Notice: Seller respects the intellectual property rights of others and take seriously compliance with its responsibilities under the Digital Millennium Copyright Act ("DMCA"). If you are a copyright owner or an agent of a copyright owner and believe that any content hosted or transmitted by Seller infringes upon your copyrights, you may submit a notification pursuant to the DMCA by contacting Seller's Copyright Agent at abuse@highland-networks.com. You acknowledge that if you fail to comply with all of the below requirements, your DMCA notice may not be valid. You must provide the following information in writing (see 17 U.S.C § 512(c)(3) for further detail):

1. An electronic or physical signature of the person authorized to act on behalf of the owner of the copyright or other right being infringed;
2. A description of the copyright-protected work or other intellectual property right that you claim has been infringed;
3. A description of the material that you claim is infringing and where it is located;
4. Your address, telephone number, and email address;
5. A statement by you that you have a good faith belief that the use of those materials is not authorized by the copyright owner, its agent, or the law; and
6. A statement by you that the above information in your notice is accurate and that, under penalty of perjury, you are the copyright or intellectual property owner or authorized to act on the copyright or intellectual property owner's behalf.

Counter-Notice: With respect to any content that was removed or disabled as a result of a notice of copyright infringement, if Customer believes that its content is not infringing or that it has authorization—from the copyright owner, the copyright owner's agent, or otherwise pursuant to the law—to post and use the content, Customer may send a counter-notice to Seller's Copyright Agent. The counter-notice must include the following information (see 17 U.S.C. § 512(g)(3) for further detail):

1. An electronic or physical signature of the Customer;
2. Identification of the material that has been removed or to which access has been disabled, and the location at which the material appeared before it was removed or access to it was disabled;
3. A statement under penalty of perjury that the Customer has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled;
4. The Customer's name, address, and telephone number, and a statement that the Customer consents to the jurisdiction of Federal District Court for the judicial district in which the address is located, or if the Customer's address is outside of the United States, for any judicial district in which the service provider may be found, and that the Customer will accept service of process from the person or agent of the person who provided the notification.

When Seller's Copyright Agent receives a counter-notice, Seller may send a copy of the counter-notice to the original complaining party informing that party that Seller may, in 10 business days, replace the removed content or stop disabling it. Unless the copyright owner files an action seeking a court order against the provider of the content, the removed content may be replaced or access to it restored, in 10 to 14 business days or more after receipt of the counter-notice, in Seller's sole discretion.

Repeat Infringer Policy: Seller's policy is to: (i) remove or disable access to material, upon notice from a third party, that is being made available through the IP Services; and (ii) in appropriate circumstances, to terminate the accounts of and block access to the IP Services by any Customer who repeatedly or egregiously infringes copyrights or other intellectual property rights.