Acceptable Use Policy

LightWave Networks, Inc. and its affiliates (hereafter "LightWave", we, us, or our) are dedicated to providing our customers (hereafter "Customer", you, or your) with a quality Service while complying with all applicable laws and maintaining a high ethical standard. Our Acceptable Use Policy ("AUP") contained herein is incorporated by this reference into the LightWave Master Service Agreement ("MSA") and any other applicable contracts that constitute the Agreement as defined in the applicable LightWave MSA. Any term not specifically defined in this AUP shall have the meaning given to it in the Agreement.

1. Modification and Acceptance. We reserve the right to amend or modify this AUP at any time. The current, in-effect AUP will be posted on our website at https://www.lightwavenetworks.com/aup. Continued use of our Services will constitute your acceptance of the in-effect AUP. It is your responsibility to ensure that your customers and users (collectively, "End Users") comply with this AUP. All violations of this policy by your End Users shall be the responsibility of the Customer.
2. Violation of AUP. Failure to abide by the terms of this AUP shall be grounds for immediate Service suspension or termination for cause. Such Service suspension or termination for cause may occur without notice in the sole discretion of LightWave. Due to the evolving nature of the Internet, the provisions of this AUP are intended as guidelines and are not meant to be a complete, exhaustive list of unacceptable uses. Generally, any conduct that violates law, regulation, or the generally accepted norms of the Internet community is prohibited whether or not it is explicitly defined herein. LightWave reserves the right in its sole discretion to determine whether an activity is acceptable or not.
3. Explicitly Prohibited Activities.
   3.1. Illegal Activities. LightWave Services may be used for lawful purposes only. Any use of a LightWave Service that is in violation of any applicable law or regulation is prohibited. The list below of such violations is intended as a guide for you and your End Users, and does not represent a complete list of all activities that represent an unlawful use of a LightWave Service.
      3.1.1. Drug dealing and/or the promotion of drug dealing activities.
      3.1.2. The storage, transmission or distribution of pirated materials.
      3.1.3. Any violation of copyright law or the intellectual property rights of others including but not limited to trademark infringement or the dissemination of trade secrets without proper authorization.
      3.1.4. Illegal gambling, lottery sites, or similar activities such as Ponzi schemes or pyramid schemes.
      3.1.5. Illegal arms trafficking.
      3.1.6. Promoting violence or injury including but not limited to threatening bodily harm or damage to an individual or group of individuals.
      3.1.7. Violation of any applicable law pertaining to computers and networks such as the creation or sending of Internet viruses, worms, or Trojan horses, flood or mail bombs, using the Service to engage in denial of service attacks, hacking, subverting and/or assisting in the subverting of the security or integrity of any company's or individual's systems, services, or networks.

3.1.8. Violating any US or international export control laws, economic sanctions, and/or restrictions, including those administered by the US Department of the Treasury's Office of Foreign Assets Control (OFAC).

3.1.9. Forging, misrepresenting, omitting or deleting message headers, return mailing information, or internet protocol addresses to conceal or misidentify the origin of a message.

3.1.10. Port scanning and exploit scanning of Internet IP addresses without the explicit consent of the owner of the IP addresses.

3.1.11. Storing, transmitting, or distributing child sexual abuse material or any other content that is obscene or otherwise unlawful.

3.1.12. Defamation, harassment, stalking, or the transmission of threatening or abusive material.

3.1.13. Fraudulent activities, including phishing, identity theft, impersonation of any person or entity, and deceptive offers.

3.1.14. Collecting, storing, or disclosing the personal information of others in violation of applicable privacy or data protection laws.

3.2. Unsolicited Commercial Email (UCE) – Spam. In addition to any other remedy available to LightWave under this AUP or the Agreement, Customer shall pay LightWave a clean-up fee of $500 per incident for each violation of this Section 3.2, payable within seven (7) days of the date of LightWave's invoice. Unpaid fees may be referred to a collection agency.

3.2.1. Prohibited Email. The sending of Unsolicited Commercial Email using any LightWave Service is strictly prohibited. The only email marketing activities allowed under this AUP are those activities compliant with the CAN-SPAM Act of 2003 (15 U.S.C. § 7701 et seq.) and all other applicable anti-spam laws. Prior to engaging in any email marketing activities using any Service provided by LightWave, it is your responsibility to familiarize yourself with the CAN-SPAM Act and all other applicable anti-spam laws. Certain activities permitted by the CAN-SPAM Act can still be violations of this AUP for other reasons as may be defined herein.

3.2.2. Hosting UCE Target Content. The sending of Unsolicited Commercial Email using another service provider is prohibited where the contents of the email advertise a website or email address, or utilize any resources, that are served through the LightWave Service. All bulk email sent whether using a LightWave Service, or the service(s) of any other provider must be solicited, which shall mean that the sender has an existing and provable relationship with the email recipient and the recipient has not requested to not receive future mailings from the sender. It is the responsibility of the Customer to maintain documentation of the relationship between the sender and recipient to provide to LightWave upon request.

3.2.3. Spam is strictly prohibited under this AUP. An electronic message is "spam" if: (1) the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; (2) the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent; and (3) the transmission and reception of the message appears to the recipient to give a disproportionate benefit to the sender. LightWave reserves the right to determine, in our sole discretion, what constitutes a violation of this spam policy. The list below of such

spam violations is intended as a guide for you and your End Users, and does not represent a complete list of all activities that LightWave may interpret as spamming.

3.2.3.1. Unsolicited or unauthorized advertising and promotional materials such as "junk mail," unsolicited instant messages, or "chain letters."

3.2.3.2. Subscribing email addresses to any mailing list without the express and verifiable permission of the email address owner is prohibited. All mailing lists run by Customer or its End Users must be closed-loop ("Confirmed Opt-in"). If a Customer cannot provide positive and verifiable proof of such consents and opt-in elections, LightWave will consider the list mailing to be unsolicited. Any Customer-maintained mailing list must also allow any party on the list to remove itself automatically and permanently.

3.2.3.3. Use of our network for the receipt of replies to spam, as defined herein.

3.2.3.4. Forgery of email headers on any email sent using the LightWave network (spoofing).

3.2.3.5. Configuration of a mail server to accept and process third-party messages for sending without user identification and authentication.

3.2.3.6. Hosting web pages that are the target of any link within any spam email, as defined herein, sent using the services of another provider.

3.2.3.7. Hosting web pages or providing services that support spam.

3.2.3.8. Advertising, transmitting, or otherwise making available any software, program, product, or service that is designed to violate this AUP or the acceptable use policy of any other Internet service provider, including, but not limited to, the facilitation of the means to send Unsolicited Commercial Email, initiation of pinging, flooding, mail-bombing, or denial of service attacks.

4. Security. This AUP also prohibits any actions that compromise our system and/or network security, the security of our customers, and that of the Internet generally. We reserve the right to immediately suspend or terminate your Services, without notice, as a result of such actions by you or your End Users. You may also be exposed to criminal and civil liability based on your actions. Examples of such actions include, but are not limited to, unauthorized access, use, probe, or scan of a system security or authentication measure, data or traffic; interference with service to any user, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks; monitoring or intercepting data or traffic on any network or system without authorization; operating open mail relays or open proxies; announcing or using IP addresses or routes not assigned to you; and forging of any TCP/IP packet header or any part of the header information in an email or a newsgroup posting.
5. Violations and Cooperation. LightWave has no obligation to monitor the Services, but reserves the right to investigate any suspected violation of this AUP and to take any action it deems appropriate, including removing or disabling access to any material that LightWave believes violates this AUP. LightWave may cooperate with law enforcement authorities, regulators, and other network operators in investigating suspected violations, and may disclose Customer information as required by law or legal process. LightWave will respond to notices of alleged copyright infringement in accordance with the Digital Millennium Copyright Act (17 U.S.C. § 512).
6. Customer Security Responsibilities. You acknowledge that the Internet can be an insecure environment. You are responsible for ensuring the security of your data, passwords, usernames,

and confidential information, and for maintaining reasonable security measures on all systems, devices, and equipment that you or your End Users connect to the LightWave network.