Acceptable Use Policy

This Acceptable Use Policy ("AUP") describes activities prohibited on the Tigunia network for the protection of Tigunia and its Representatives, Services, network, and other Clients. Questions regarding this policy should be directed to support@Tigunia.com.

- **Abuse**. Client shall not use Tigunia's Services or network to engage in, foster, solicit, or promote illegal, abusive, or irresponsible behavior, including without limitation:

    - Conduct likely to breach any laws, codes, or regulations applicable to the parties (including conduct infringing or misappropriating intellectual property, trade secrets, confidential or proprietary information; or which is fraudulent, unfair, deceptive or defamatory);
    - Unauthorized access to, monitoring or use of, or interference with an internet account, computer, systems, networks, data, or traffic;
    - Intentionally, knowingly, or recklessly introducing any malicious code into the Services;
    - Conduct violating rules and conventions of any domain registrar, email service, bulletin board, chat group, or forum used in conjunction with Tigunia Services or network (including using false, misleading, or deceptive TCP-IP packet header information in an email or newsgroup posting);
    - Deceitfully collecting, transmitting, or using information, or distributing software which covertly gathers or transmits information about a user;
    - Distributing advertisement delivery software unless the user affirmatively consents to the download and installation of same based on clear and conspicuous notice of the nature of the software, and where the user can easily remove software using standard tools included on major operating systems;
    - Conduct likely to result in retaliation or adverse action against Tigunia or its services, network, website or Representatives (including efforts that result in the listing of the Tigunia IP space on an abuse database);
    - Conduct intended to withhold or cloak identity or contact information, registering to use the Services under a false name, or using an invalid or unauthorized credit card in connection with the Services;
    - Gambling activity that violates any applicable codes of practice, required licenses or technical standards;
    - Use of any Tigunia provided shared system in a way that unnecessarily interferes with the normal operation of the shared system, or consumes a disproportionate share of the system resources; and,
    - Conduct that creates a risk to safety or health, national security, or law enforcement.

- **Offensive Behavior.** Client shall not be abusive or offensive to Tigunia Representatives. Client shall not publish, transmit, or store on or via the Services, content or links to content

that Tigunia reasonably believes relates in any manner to child pornography, bestiality, non-consensual sex acts, or live sex acts; or is excessively violent, incites or threatens violence, contains harassing content or hate speech, violates a person's privacy, is malicious or morally repugnant.

- **No High-Risk Use.** Client shall not use the Services in any situation where the failure or fault of the Services could lead to death or serious bodily injury of any person, or to physical or environmental damage (including in connection with aircraft or other modes of human mass transportation, or nuclear or chemical facilities).

- **Mail Requirements.** For bulk or commercial email sent by or on behalf of Client using the Services or from any network that directly or indirectly refers recipients to a site hosted using the Services (including using third party distribution lists), Client shall:

    - Post a privacy policy for each associated domain;
    - Post an email address for complaints in a conspicuous place on any associated website, promptly respond to messages sent to that address, and have means to track anonymous complaints;
    - Obtain affirmative consent to receive e-mail from intended recipients using reasonable means to verify the ownership of the e-mail address, honor and notify recipients of consent revocation, and evidence consent within 72 hours of the recipient or Tigunia request; and,
    - Include the recipient's e-mail address in the e-mail body or "TO" line.

- **Vulnerability Testing.** Client shall not attempt to test the vulnerability of a Tigunia system or network, or attempt to breach Tigunia security measures, by any means (Client may conduct vulnerability testing of their Hosted System only with Tigunia' prior written consent).

- **Export Control.** Client shall ensure that the Services are not used in the breach of export laws, controls, regulations or sanction policies of the United States or Client's applicable jurisdiction. Client shall ensure Services are not used by any person or entity suspected of involvement or affiliation with those involved in activities or causes relating to: human trafficking; illegal gambling; terrorism; narcotics trafficking; arms trafficking or the proliferation, development, design, manufacture, production, stockpiling, or use of nuclear, chemical, or biological weapons, weapons of mass destruction, or missiles.

- **Cooperation with Investigations and Proceedings.** Client agrees that Tigunia may permit a relevant authority to inspect Client's content or traffic if Tigunia is legally required to do so, provided Tigunia gives Client reasonable prior notice (where permitted by applicable law and regulation). Tigunia may report to the appropriate authorities any Client conduct that

Tigunia believes violates applicable law without notice to Client (including providing any information about Client, its users or traffic). Tigunia may cooperate in response to a formal request from a law enforcement or regulatory agency investigating conduct that Tigunia believes violates applicable law, or in a civil action that on its face meets the requirements for such a request.

- **Domain Names, IP Addresses, and DNS Records.** Client shall maintain valid information with the Client's domain name registrar for any domain that is hosted on the Tigunia network, and only use IP addresses assigned to Client by Tigunia in connection with the Services. Client agrees that Tigunia may modify, transfer, or delete any DNS record or zone on Tigunia managed or operated DNS servers or services upon request from the registrant or administrative contact according to the registrar's WHOIS system.

- **Changes to AUP.** Tigunia may amend this AUP by publishing a revised version at www.Tigunia.com. The revised AUP shall become effective as to Client upon publication.

- **AUP Breach.** If Client breaches the AUP (including unintentionally, resulting from Client's failure to use reasonable security precautions, or as a result of activity that is occurring without Client authorization), Tigunia may block any content or traffic, suspend the Services, or terminate the Services in accordance with the Agreement. No credit shall be available under any Service Level Agreement for interruptions of Services resulting from an AUP breach. Client's use of the Services to assist another person in an activity that would breach this AUP if performed by Client is an AUP breach.