**Medistry LLC (.med) Acceptable Use Policy (AUP)**

.med provides an abuse point of contact through an e-mail address (abuse@medistry.med).

Registrant will comply with all applicable registration agreements, including applicable terms of the .med registry agreement with ICANN and the applicable registrar agreement. .med reserves the right, at its sole discretion and at any time and without limitation, to deny, suspend, cancel, redirect, or transfer any registration or transaction, or place any domain name(s) on registry lock, hold, or similar status as it determines necessary for any of the following reasons:

- to protect the integrity and stability of .med;
- to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process;
- to avoid any liability, civil or criminal, on the part of .med, its affiliates, subsidiaries, officers, directors, contracted parties, agents, or employees;
- to comply with the terms of all applicable registration agreements and .med policies;
- where registrant fails to keep RDAP information accurate or up-to-date;
- domain name use is abusive or violates this AUP, or a third party's rights or acceptable use policies, including but not limited to the infringement of any copyright or trademark;
- to correct mistakes made by a registry operator or any registrar in connection with a domain name registration; or
- as needed during resolution of a dispute.

Abusive use of a domain is described as an illegal, disruptive, malicious, or fraudulent action and includes, without limitation, the following:

- distribution of malware;
- dissemination of software designed to infiltrate or damage a computer system without the owners informed consent, including, without limitation, computer viruses, worms, keyloggers, trojans, and fake antivirus products;
- phishing, or any attempt to acquire sensitive information such as usernames,
- passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication;
- DNS hijacking or poisoning;
- spam, including using electronic messaging systems to send unsolicited bulk messages,

- including but not limited to e-mail spam, instant messaging spam, mobile messaging spam, and the spamming of Internet forums;
- botnets, including malicious fast-flux hosting;
- denial-of-service attacks;
- child pornography or any images of child abuse;
- promotion, encouragement, sale, or distribution of prescription medication without a valid prescription in violation of applicable law and;
- Illegal access of computers or networks