.spa
YOUR ONLINE SANCTUARY

ANTI ABUSE POLICY

1. Abuse

Abusive use(s) of domain names within .SPA TLD should not be tolerated. The nature of such abuses creates security and stability issues for the registry, registrars and registrants, as well as for users of the Internet in general. The Registry defines abusive use as the wrong or excessive use of power, position or ability, and includes, without limitation, the following:

- Illegal or fraudulent actions;
- Spam: The use of electronic messaging systems to send unsolicited bulk messages. The term applies to e-mail spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of Websites and Internet forums. An example, for purposes of illustration, would be the use of email in denial-of-service attacks;
- Phishing: The use of counterfeit Web pages that are designed to trick recipients into divulging sensitive data such as usernames, passwords, or financial data;
- Pharming: The redirecting of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning;
- Willful distribution of malware: The dissemination of software designed to infiltrate or damage a computer system without the owner's informed consent. Examples include, without limitation, computer viruses, worms, keyloggers, and trojan horses;
- Fast flux hosting: Use of fast-flux techniques to disguise the location of Websites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities. Fast-flux techniques use DNS to frequently change the location on the Internet to which the domain name of an Internet host or name server resolves. Fast flux hosting may be used only with prior permission of The Registry;
- Botnet command and control: Services run on a domain name that are used to control a collection of compromised computers or "zombies," or to direct denial-of-service attacks (DDoS attacks);
- Distribution of child pornography; and
- Illegal Access to Other Computers or Networks: Illegally accessing computers, accounts, or networks belonging to

another party, or attempting to penetrate security measures of another individual's system (often known as "hacking"). Also, any activity that might be used as a precursor to an attempted system penetration (e.g., port scan, stealth scan, or other information gathering activity).

Consequences for such activities including suspension of the domain name.

2. **Registration Agreement**

Pursuant to the Registration Agreement, The Registry reserve the right to deny, cancel, or transfer any registration or transaction, or place any domain name(s) on registry lock or hold, in its discretion, if a domain is found to violate this anti abuse policy, with the aim to:

- Protect the security and stability of the DNS;
- Comply with any applicable court order, laws, government rules and requests of law enforcement;
- Comply with any dispute resolution process;
- Comply with the terms of Registration Agreement;
- Avoid any liability, civil or criminal, on the part of the registry, as well as its affiliates, subsidiaries, officers, directors and employees;
- Correct mistakes of the registry or any registrars with regards to registry TLD domain registration.

The Registry reserves the right to place upon registry lock, hold or similar status a domain name during resolution of a dispute.