This Acceptable Use Policy gives the Registry the ability to lock, cancel, transfer or take ownership of any .ooo gTLD domain name, either temporarily or permanently, if the domain name is being used in a manner that appears to threaten the stability, integrity or security of the Registry, or any of its registrar partners – and/or that may put the safety and security of any registrant or user at risk. The process also allows the Registry to take preventive measures to avoid any such criminal or security threats.

The Acceptable Use Policy may be triggered through a variety of channels, including, among other things, private complaint, public alert, government or enforcement agency outreach, and the on-going monitoring by the Registry or its partners. In all cases, the Registry or its designees will alert Registry's registrar partners about any identified threats, and will work closely with them to bring offending sites into compliance.

The following are some (but not all) activities that may be subject to rapid domain compliance:

- ***Phishing:** the attempt to acquire personally identifiable information by masquerading as a website other than your own.*
- ***Pharming:** the redirection of Internet users to websites other than those the user intends to visit, usually through unauthorized changes to the Hosts file on a victim's computer or DNS records in DNS servers.*
- ***Dissemination of Malware:** the intentional creation and distribution of "malicious" software designed to infiltrate a computer system without the owner's consent, including, without limitation, computer viruses, worms, key loggers, and Trojans.*
- ***Fast Flux Hosting:** a technique used to shelter Phishing, Pharming and Malware sites and networks from detection and to frustrate methods employed to defend against such practices, whereby the IP address associated with fraudulent websites are changed rapidly so as to make the true location of the sites difficult to find.*
- ***Botnetting:** the development and use of a command, agent, motor, service, or software which is implemented: (1) to remotely control the computer or computer system of an Internet user without their knowledge or consent, (2) to generate direct denial of service (DDOS) attacks.*
- ***Malicious Hacking:** the attempt to gain unauthorized access (or exceed the level of authorized access) to a computer, information system, user account or profile, database, or security system.*
- ***Child Pornography:** the storage, publication, display and/or dissemination of pornographic materials depicting individuals under the age of majority in the relevant jurisdiction.*

The Registry reserves the right, in its sole discretion, to take any administrative and operational actions necessary, including the use of computer forensics and information security technological services, among other things, in order to implement the Acceptable Use Policy. In addition, the Registry reserves the right to deny, cancel or transfer any registration or transaction, or place any domain name(s) on registry lock, hold or similar status, that it deems necessary, in its discretion; (1) to protect the integrity and stability of the registry; (2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of Registry as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement or (5) to correct mistakes made by the Registry or any Registrar in

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