Anti-Abuse Policy

Desi Networks, LLC

Version 1, March 2014

The .desi registry ("Registry") adopts certain content and acceptable usage policies and any violations of these would be treated as abuse. .desi domain names shall not be used to: transmit, distribute, disseminate, publish or store any information that is in violation of any applicable law or regulation or is defamatory, abusive, obscene, indecent, or harassing, or that threatens or encourages injury to persons or property or infringement of the lawful rights of any party. Specifically, the following are deemed, without limitation, as violations of our acceptable usage policy

1. Intellectual Property, Trademark, Copyright, and Patent Violations, including Piracy
Intellectual property (IP) is a term referring to a number of distinct types of creations of the mind for which a set of exclusive rights are recognized – and the corresponding fields of law. Under intellectual property law, owners are granted certain exclusive rights to a variety of intangible assets, such as musical, literary, and artistic works; discoveries and inventions; and words, phrases, symbols, and designs. Common types of intellectual property rights include copyrights, trademarks, patents, industrial design rights and trade secrets in recognized jurisdictions. Any act resulting in theft, misuse, misrepresentation or any other harmful act by any individual or a company is categorized as Intellectual Property violation.

2. Spamming
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 Web sites and Internet forums. Unsolicited emails advertising legitimate and illegitimate products, services, and⁄or charitable requests and requests for assistance are also considered as spam.

3. Phishing (and various forms of identity theft)
Fraudulent web services and applications meant to represent⁄confuse or mislead internet users into believing they represent services or products for nefarious purposes, such as illegally gaining login credentials to actual legitimate services.

4. Pharming and DNS Hijacking
Redirection of DNS traffic from legitimate and intended destinations, by compromising the integrity of the relevant DNS systems. This leads unsuspecting Internet users to fraudulent web services and applications for nefarious purposes, such as illegally gaining login credentials to actual legitimate services.

5. Distribution Of Viruses Or Malware
Most typically the result of a security compromised web service where the perpetrator has installed a virus or "malevolent" piece of software meant to infect computers attempting to use the web service in turn. Infected computers are then security compromised for various nefarious purposes such as gaining stored security credentials or personal identity information such as

credit card data. Additionally compromised computers can sometimes be remotely controlled to inflict harm on other internet services.

6. Child Pornography
Child pornography refers to images or films (also known as child abuse images) and, in some cases, writings depicting sexually explicit activities involving a minor.

7. Using fast flux techniques
A methodology for hiding multiple source computers delivering malware, phishing or other harmful services behind a single domain hostname, by rapidly rotating associated IP addresses of the sources computers through related rapid DNS changes. This is typically done at DNS zones delegated below the level of a TLD DNS zone.

8. Running botnet command and control operations
A Botnet is a significant coordinated net of compromised (sometimes tens of thousands) computers running software services to enact various forms of harm – ranging from unsanctioned spam to placing undue transaction traffic on valid computer services such as DNS or web services. Command and control refers to a smaller number of computers that issue/distribute subsequent commands to the Botnet. Compromised botnet computers will periodically check in with a command and control computer that hides behind a list of date triggered, rotating domain registrations, which are pre-loaded in the compromised computer during its last check-in.

Registries play a key role in breaking this cycle of pre-determined domain registrations by deactivating said registrations prior to the compromised computers being able to use them to contact the command and control computer. Successful intervention results in the botnet losing contact with their command and control computers, leaving them inactive and reducing potential harms.

9. Hacking
Hacking constitutes illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of other individuals. Also includes any activity that might be used as a precursor to an attempted system penetration.

10. Financial and Other Confidence Scams
Financial scams, including but not limited to the cases defined below, are operated by fraudsters to lure investors into fraudulent money making schemes. Prominent examples that will be treated as abusive are:

1. Ponzi Schemes: A Ponzi scheme is essentially an investment fraud wherein the operator promises high financial returns or dividends that are not available through traditional

investments. Instead of investing victims' funds, the operator pays dividends to initial investors using the principle amounts invested by subsequent investors. The scheme generally falls apart when the operator flees with all of the proceeds, or when a sufficient number of new investors cannot be found to allow the continued payment of dividends

2. Money Laundering: Money laundering, the metaphorical cleaning of money with regard to appearances in law, is the practice of engaging in specific financial transactions in order to conceal the identity, source, and⁄or destination of money, and is a main operation of the underground economy
3. 419 Scams: 419 scam (aka Nigeria scam or West African scam) is a type of fraud named after an article of the Nigerian penal code under which it is prosecuted. It is also known as Advance Fee Fraud. The scam format is to get the victim to send cash (or other items of value) upfront by promising them a large amount of money that they would receive later if they cooperate

11. Illegal Pharmaceutical Distribution

Distribution and promotion of drugs, locally within a nation or overseas, without prescription and appropriate licenses as required in the country of distribution are termed illegal.

12. Other Violations

Other violations that will be expressly prohibited under the Registry policies, include:

- Maintaining inaccurate contact details on the WHOIS
- Network attacks
- Libelous or defamatory content adjudicated by a competent court of law
- Illegal Adult/Pornographic content
- Content that violates any privacy right
- Internet relay chat servers ("IRCs") IRC bots
- Distribution of malicious tools promoting or facilitating hacking, unsolicited bulk emails or sms, fake anti-malware products, phishing kits, unauthorized data banks violating individual privacy rights
- Content which violates any export, re-export or import laws and regulations of any jurisdiction
- Not publicly offer, advertise, or otherwise make available the delegation of sub-domains from the Domain Name
- Violation of any federal, state or local rule, regulation or law, or for any unlawful purpose, or in a manner injurious to the .desi Registry, its service providers and partners, or their reputation, including but not limited to the above mentioned activities mentioned as part of this policy

Reservation Of Rights

The Registry expressly reserves the right to deny, cancel, suspend, lock or transfer any Domain Name registration that it deems necessary in its discretion: (i) to protect the integrity and stability of the Registry; (ii) to comply with any applicable laws, government rules or requirements, requests of law enforcement; (iii) in the event a Domain Name is used in violation of these policies and any other policies regarding .desi and; (iv) in compliance with any dispute resolution process, or to avoid any liability, civil or criminal, on the part of Registry and its affiliates, licensors subsidiaries, officers, directors and employees.