Radix – Acceptable Use and Anti-Abuse Policy

I. General Provisions

1. Radix Domain Solutions Pte. Ltd and its subsidiaries ("Radix") are committed to the stable and secure operation of its top-level domains ("TLDs"). Abusive use of domain names creates security and stability issues for registries, registrars and registrants – as well as for users of the Internet in general. Accordingly, Radix requires that every domain name in its TLDs ("Registered Name") and Registered Name Holder adhere to this Acceptable Use and Anti-Abuse Policy ("AUP"). For the purpose of this AUP, a "Registered Name Holder" refers to the person or company owning or otherwise controlling a Registered Name by virtue of a registration agreement with a registrar.

2. Every Registered Name Holder is required to enter into and comply with a registration agreement with an ICANN-Accredited registrar or its authorized representative.

3. Every Registered Name Holder is required to comply with all ICANN consensus policies applicable to Registered Name Holders, including (a) the Uniform Domain Name Dispute Resolution Policy (http://www.icann.org/en/help/dndr/udrp), and (b) the Uniform Rapid Suspension Policy (http://newgtlds.icann.org/en/applicants/urs), and (c) such other ICANN consensus policies as ICANN publishes on its website and makes applicable to Radix, Registrars or Registered Name Holders, and as may be amended by ICANN from time to time.

4. Every Registered Name Holder acknowledges and agrees that Registered Name Holders are solely responsible for the content they publish on websites on the Registered Name. Radix cannot and does not design, review or screen content on any web site and does not assume any obligation to monitor such content. However, each Registered Name Holder agrees that Radix may review web sites or other content in responding to a third-party complaint or for any other reason.

5. By applying for or obtaining a Registered Name, every Registered Name Holder acknowledges, accepts and agrees to comply with the terms under which such application and registration was made, including the terms and conditions of all other applicable policies available on the Radix website and use restrictions set forth herein.

6. Registered Name Holders who have obtained or registered any two character second level domain name/s under any of the TLDs will take steps to ensure against misrepresenting or falsely implying that the Registered Name Holder or its business is affiliated with a government or country-code manager if such affiliation, sponsorship or endorsement does not exist.

7. Radix reserves the right to deny, suspend, cancel, redirect or transfer any registration or transaction, or place any Registered Name(s) on registry lock, hold or similar status that it deems necessary, in its sole discretion, for any of the following reasons:

(a) to protect the integrity and stability of the registry;

(b) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process;

(c) to avoid any liability, civil or criminal, on the part of Radix, as well as its affiliates, subsidiaries, officers, directors, contracted partied, agents or employees;

(d) to comply with the terms of the applicable registration agreement and Radix policies;

(e) where the Registered Name Holder fails to keep Whois information accurate or up-to-date;

(f) Registered Name use is abusive or violates the AUP, or a third party's rights or acceptable use policies, including but not limited to the infringement of any copyright or trademark;

(g) where the Registered Name is found to have been registered as part of a set of any pattern based registration which has shown abusive trends in the past, or is part of a present or ongoing abusive campaign, including but not limited to domains registered using any domain generation algorithms, scripts, dictionaries, etc, whether detected by Radix or a registrar;

(h) to correct mistakes made by Radix or any registrar in connection with the registration of a Registered Name; or

(i) as needed during resolution of a dispute.

8. Radix reserves the right to disclose individual non-public personal data of Registered Name Holders associated with Registered Names which are found to be in violation of this AUP and/or if required or requested by law enforcement agencies, security agencies, registries, registrars and other service providers irrespective of the number and frequency of AUP violations.

II. Prohibited Uses

The following will be deemed as violations of the AUP:

1. Intellectual property, Trademark, Copyright, and Patent violations, including piracy

   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 Registered Name

Holder will be categorized as an Intellectual Property violation.

2. Spamming

   Spamming refers to 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

   This includes 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. 3

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 source 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.

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.″

    1. 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.

    2. 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. SEO Poisoning

    SEO Poisoning, also known as search poisoning, is an attack method in which cybercriminals create malicious websites and use search engine optimization tactics to make them show up more prominently in search results.

13. Sale of Fake / Counterfeit Products

    This includes creation of storefronts or websites selling / offering or purporting to sell /offer any fake or counterfeit products or services.

14. Other violations

    Other violations that will be expressly prohibited under the TLDs include

    1. Network attacks
    2. Violation of applicable laws, government rules and other usage policies

III. Reporting violations / abuse

Radix provides an abuse point of contact through an e-mail address posted on the Radix website found at https://radix.website/report-abuse Radix also provides a web form for complaints on the Radix website.

IV. Managing violations and abuse

Radix will address abusive behaviour in its TLDs consistent with this AUP.

1. Radix shall have the discretion to undertake such actions as cancellation transfer, locking, or suspension of a Registered Name subject to abusive uses. Such abusive uses create security and stability issues for Radix, registrars and Registered Name Holders, as well as for users of

the Internet in general. Radix defines abusive use as the wrong or excessive use of power, position or ability, and includes, without limitation, all the uses cited under “Prohibited Uses” above.

2. Radix also reserves the right to deny new registrations and/or suspend existing registrations of names to a Registered Name Holder who has repeatedly violated the terms of this AUP in any TLD, or has been identified as a known abuser or criminal by any law enforcement agency or government whether or not the violations were committed in relation to the use of a domain name or an internet transaction. Registered Name Holders, their agents or affiliates found through the application of this AUP to have repeatedly engaged in abusive use of Registered Names may be disqualified from maintaining any Registered Names or making future registrations. This will be triggered when it is clear that a Registered Name Holder has violated the AUP an unusual number of times.

V. Modifications to this AUP

Radix, in its sole discretion, may modify this AUP. Any such revised policy will be posted on the Radix website at least thirty (30) calendar days before it becomes effective. Continued use of the Registered Names after the date of the modified AUP taking effect constitutes acceptance of the modification.