ACCEPTABLE USE / ANTI-ABUSE POLICY

1.0 Title: Acceptable Use / Anti-Abuse Policy

Version Control: 1.0

Date of Implementation: February 28, 2020

2.0 Summary

This document sets forth the Acceptable Use / Anti-Abuse Policy (the "Policy") that Registrants must adhere to when registering and using a domain name in the .CPA TLD, as well as outlines the reservation of rights that Registry Operator retains to address non-compliance.

3.0 Registry Operator's Reservation of Rights

Registry Operator reserves the right to deny, cancel or transfer any registration or transaction, or place any domain name on registry lock, hold or similar status, as it deems necessary, in its unlimited and sole discretion and without notice, either temporarily or permanently:

3.1 To protect the integrity, security and stability of the Domain Name system (DNS);

3.2 To comply with any applicable court orders, laws, government rules or requirements, requests of law enforcement or other governmental agency or organization, or any dispute resolution process;

3.3 To avoid any potential liability, civil or criminal, on the part of Registry Operator, as well as its affiliates, subsidiaries, officers, directors, employees and members;

3.4 To comply with the terms of the Registration Agreement;

3.5 To respond to or to protect Registry Operator and the public against any form of Prohibited Activities;

3.6 To comply with specifications adopted by any industry group generally recognized as authoritative with respect to the Internet (e.g., Requests for Comments (RFCs));

3.7 To correct mistakes made by Registry Operator, Registry Service Provider, or Registrar in connection with a domain name registration; or

3.8 For the non-payment of fees.

4.0 Prescriptive Registrant Obligations

Registrants in .CPA TLD are required to:

4.1 Comply with all applicable policies posted on Registry Operator's website at domains.cpa.com;

4.2 Comply with their Registration Agreement;

4.3 Notify Registry Operator within one (1) business day if public regulatory action has been taken against them for failure to comply with reasonable and appropriate security measures or that has resulted in the revocation of their regulatory charter or license to operate in the field of public accounting; and

4.4 Comply with the following obligations, imposed by ICANN, in connection with its Governmental Advisory Committee Advice:

4.4.1 Maintain accurate and up-to-date Whois information to receive notification of complaints or reports of registration abuse, as well as the contact details of the relevant regulatory or, industry self-regulatory bodies in their main place of business;

4.4.2 Report any material changes to the validity of Registrant's authorizations, charters, licenses and/or other related credentials for participation in .CPA TLD in order to ensure they continue to conform to appropriate regulations and licensing requirements and generally conduct their activities in the interests of the consumers they serve;

4.4.3 Comply with all applicable laws, including those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, debt collection, disclosure of data, and financial disclosure; and

4.4.4 Implement reasonable and appropriate security measures commensurate with the offering of financial data services, as defined by applicable law.

5.0 Prohibited Activities

The following is a non-exhaustive list of activities that are prohibited:

5.1 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 Distributed Denial of Service (DDoS) attacks;

5.2 Distribution of Malware: The intentional creation and intentional or unintentional distribution of “malicious” software designed to infiltrate a computer system without the owner’s consent, including, without limitation, computer viruses, worms, keyloggers, and Trojans;

5.3 Fast Flux Attacks/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 sites are changed rapidly so as to make the true location of the sites difficult to find;

5.4 Hacking: Unauthorized access to a computer network;

5.5 Phishing: The use of email and counterfeit web pages that are designed to trick recipients into divulging sensitive data such as personally identifying information, usernames, passwords, or financial data;

5.6 Pharming: The redirecting of unknown users to fraudulent sites or services, typically through, but not limited to, DNS hijacking or cache poisoning;

5.7 Spam: The use of electronic messaging systems to send unsolicited bulk messages. The term applies to email spam and similar abuses such as instant messaging spam, mobile messaging spam, and spamming of websites and Internet forums;

5.8 Man in the browser, man in the middle: The use of malicious software or compromised network facilities for fraudulent or deceptive purposes;

5.9 Activities contrary to applicable law: Including trademark or copyright infringement, fraudulent or deceptive trade practices, counterfeiting or a violation of the intellectual property right of any other person or entity;

5.10 Inappropriate content: The storage, publication, display and/or dissemination of material as defined by applicable laws and regulations in respective jurisdictions.

6.0 Registry Operator’s Response Plan

Registry Operator will maintain a public email (domains@hq.cpa.com) on its respective websites for interested third parties to submit alleged incident of abuse and/or non-compliance. Registry Operator’s plan to respond to allegations of abuse is based upon the following four pillars: Verification, Investigation, Remediation and Follow-up as identified in more detail below.

6.1 Verification

Registry Operator will use commercially reasonable efforts to review all submissions and make an initial determination regarding the source and legitimacy of each submission.

6.2 Investigation
Registry Operator will prioritize all investigations in the following order:

1.Law enforcement complaints (within 24 hours);
2. Third party security, stability or criminal complaints (within one (2) business day); and
3. Third party non-security, non-stability, or non-criminal complaints (within five (5) business days).

6.3 Remediation

As a result of any investigation involving credible complaints or violations of law in matters pertaining to security, stability or criminal activity, Registry Operator's default option will be the suspension of the domain name within twelve hours of completing an initial investigation absent exceptional circumstances. In all other complaints not involving security, stability or criminal activity, Registry Operator will seek to resolve the matter through an escalated notification process: email, telephone, certified mail.

6.4 Follow-Up
Where, as a result of a complaint, there is found to be abusive/non-compliant activity, Registry Operator will follow-up on each complaint to update the status of the domain name after the issue has been resolved. Registry Operator will also engage with the Registrant to educate them about how to avoid future remediation actions.

7.0 Amendment

Registry Operator reserves the right to modify this Policy at its sole discretion in accordance with its rights and obligations set forth in its Registry Agreement. Such revised Policy shall be posted on Registry Operator's website at domains.cpa at least 15-calendar days before its effective date.