.trust Acceptable Use Policy

NCC Group Domain Services, Inc. ("the Registry") offers this Acceptable Use Policy for the .trust gTLD. This document summarizes the process, procedures and rules applicable to the application, registration and maintenance of a domain in the .trust gTLD.

1. General

1.1. **Guidelines Only**. The provisions of this policy are intended as guidelines and are not meant to be exhaustive. Generally, conduct that violates law, regulation or the accepted norms of the Internet community, whether or not expressly mentioned in this policy, is prohibited. We reserve the right at all times to prohibit activities that damage our commercial reputation and goodwill, or the integrity of the .trust gTLD.

1.2. **Modifications**. Registry reserves the right to modify this Acceptable Use Policy at any time. Interested parties should check on the Registry Website at URL for the current version.

1.3. **Launch Timeline**. There will be an End Date Sunrise Period for 90 days beginning on December 16, 2014. This will be followed by General Availability.

1.4. **Term of Registration.** Names in .trust may be registered for a period of no less than one (1) year and no more than ten (10) years, commencing on the date on which the Registry accepts the application for registration for a .trust domain ("Registration Application") submitted by a registrar that is accredited in .trust ("Accredited Registrar"). All Registration Applications must specify the registration period (the "Term").

1.5. **Application Process**. The application process for the .trust gTLD is set forth in the .trust Administrative Framework ("Administrative Framework). A copy of the current version of the Administrative Framework is available on Registry's website at https://whodoyou.trust/resources/policies/. The Administrative Framework requires that a .trust domain be compliant with the .trust Technical Policy ("Technical Policy"). A copy of the current version of the Technical Policy is available on Registry's website at https://whodoyou.trust/resources/policies/.

2. Application Requirements

2.1. **Allowed Registrants**. Registration Applications must be submitted by the party that will operate the .trust domain ("Registrant"). Registration Applications may not be submitted by a proxy for the Registrant.

2.2. **Acceptable Domain Names**. Only names that meet each of these requirements can be registered as a .trust domain name ("Domain Name").

(a) **Available**. The Domain Name must not be:

(1) Already registered as a Domain Name;

(2) Reserved or blocked by the Registry;

(b) **Technically Qualified**. The Domain Name must meet these technical requirements:

(1) Contain a minimum of 3 characters selected from the letters "a" to "z" or "A" to "Z" in standard US ASCII character set, the digits "0" to "9" and the hyphen ("-");

(2) Contain a maximum of 63 characters (not including the ".trust" suffix);

(3) Contain at least one letter ("a" to "z" or "A" to "Z") in standard US ASCII script;

(4) Not begin or end with a hyphen ("-")

(5) Not contain a hyphen ("-") in the 3rd and 4th positions; and

(6) Not consisting purely of digits.

(c) **Registered Trademark**. As provided in the Administrative Framework, the Domain Name must be either a valid trademark to which the Registrant has the legal right to use as a domain name, or an established mark properly associated with the Registrant and the Registrant's business.

3. Sunrise Policy

3.1. The .trust Sunrise Period will be a 90-day "end date" Sunrise Period.

3.2. Qualifying applications during the Sunrise Period will be accepted on a "first come, first served" basis.

4. Prohibited Actions

Conduct in violation of this Acceptable Use Policy includes:

4.1. **Phishing** - attempting to defraud and defame Internet users by masquerading as a known website, with the intent to steal or expose credentials, money or identities;

4.2. **Domain Name or Domain Theft -** changing the registration of a domain name without the permission of its original registrant;

4.3. **Botnet Command and Control -** running services on a domain name to control a collection of compromised computers or "zombies," or to direct Distributed Denial of Service attacks ("DDoS attacks");

4.4. **Distribution of Malware -** creating and/or distributing "malicious" software designed to infiltrate a computer system, mobile device, software, operating infrastructure, and/or website, without the owner's or authorized party's consent; malware includes, without limitation, computer viruses, worms, keyloggers and trojan horses;

4.5. **Fast Flux Attacks/Hosting -** sheltering of phishing, pharming and malware sites and networks from detection, and the frustration of methods employed to defend against such practices, whereby the IP addresses associated with fraudulent sites are changed rapidly so as to make the true location of the sites difficult to find;

4.6. **Hacking -** attempting to gain unauthorized access (or exceed the level of authorized access) to a computer, information system, user account or profile, database, or security system;

4.7. **Pharming -** redirecting Internet users to websites other than those the user intends to visit, usually through, but not limited to, unauthorized changes to the Hosts file on a victim's computer or DNS records in DNS servers, or DNS hijacking or poisoning;

4.8. **Spam -** using 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;

4.9. **Piracy -** publishing, displaying and/or disseminating without license or rights any material that infringes the copyrights of any person or entity;

4.10. **Counterfeiting -** selling and advertising illegal goods, including without limitations, goods that infringe the trademarks of any party;

4.11. **Child Pornography -** storing, publishing, displaying and/or disseminating pornographic materials depicting individuals under the legal age in the relevant jurisdiction; in addition, no website hosted on any .trust domain may be used in a way as to mislead or deceive minors into viewing sexually explicit materials, whether in violation of a governing law or otherwise;

4.12. **Other Conduct** - Further conduct in violation of the Acceptable Use Policy includes, but is not limited to: cybersquatting; front-running; operating gripe sites; using deceptive and/or offensive domain names; issuing fake renewal notices; running cross-gTLD registration scams; engaging in name spinning, pay-per-click, traffic diversion, false affiliation, domain kiting/tasting, fast-flux, or 419 scams; using the domain name in a manner that threatens or 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.

5. Privacy

Registry will not sell or commercially-distribute any personal information obtained from Registrant to any third party without Registrant's express consent, or use such personal information for any purpose other than the operation of the .trust registry and to comply with laws and other legal obligations. For more information on privacy, see the NCC Group Domain Services Privacy Policy, which may be found at https://whodoyou.trust/resources/policies/, and which is incorporated by this reference.

6. Registrant's Obligations

At all times that Registrant is registered with Registry, Registrant will:

6.1. Comply with the requirements of the Administrative Framework and the Technical Policy;

6.2. Keep secure and not disclose any password which may be given to Registrant by Registry to third parties and only use any such passwords will for the purposes authorized by Registrar; Registrant will notify Registry immediately of any known or suspected unauthorized use of the password; Registrant will be liable for any unauthorized use of Registrant's password;

6.3. Respect the privacy of others, and not send unsolicited, harassing, slanderous or threatening content;

6.4. Not use any names, documents, pictures or other elements of Registry's website so as to create the impression of any relationship whatsoever with any of Registry's products or

services, or of support for any of Registry's products or services without the prior written consent of Registry; and

6.5. Treat all confidential and proprietary information and documents provided to Registrant by Registry as confidential, and not disclose the same to a third party except with Registrant's express consent, or if required by law.

7. Enforcement

7.1. **Policies**. The Registry reserves the right, in its sole discretion and without notice to any other party, to take appropriate actions (whether administrative, operational or otherwise) in order to accomplish any or all of the following:

(a) Protect the integrity and stability of the Registry;

(b) Enforce the procedures and requirements of the Administrative Framework and the Technical Policy;

(c) Comply with any applicable laws, government rules or requirements, ICANN regulations, requests of law enforcement, or any dispute resolution process;

(d) Avoid any liability, civil or criminal, on the part of Registry as well as its affiliates, subsidiaries, officers, directors, and employees;

(e) Comply with the terms of the registration agreement between Registrant and Registrar, the Registry-Registrar Agreement between Registry and its accredited registrars, the Registry Agreement between Registry and ICANN, or any other binding commitments, whether written or otherwise;

(f) Correct mistakes made by the Registry or any Registrar in connection with a domain name registration;

(g) Respond to complaints of abusive behavior on websites hosted on .trust domains; or

(h) Otherwise implement the Acceptable Use Policy.

7.2. **Enforcement Actions**. To enforce this Acceptable Use Policy, including responding to any prohibited activities or to effectuate the policy purposes described above, the Registry may take any or all of the following actions:

(a) Conduct an assessment to determine whether any alleged abusive or otherwise harmful behavior violates the Registry's policies, applicable laws, or ICANN regulations;

(b) Lock down a domain name preventing any changes to the contact and name server information associated with the domain name;

(c) Place a domain name "on hold" rendering the domain name nonresolvable or transferring the domain name to another Registrar;

(d) Substitute name servers in cases in which the domain name is associated with an existing law enforcement investigation in order to collect information about the DNS queries and when appropriate, we will share information with law enforcement to assist the investigation;

(e) Cancel or transfer or take ownership of any domain name, either temporarily or permanently;

(f) Deny attempted registrations from repeat violators;

(g) Use relevant technological services, whether our own or third party, such as computer forensics and information security;

(h) Share relevant information on abuse with other registries, Registrars, ccTLDs, law enforcement authorities (i.e., security professionals, etc.) not only on abusive domain name registrations within its own gTLD, but also information uncovered with respect to domain names in other registries to enable such parties to take appropriate action; and

(i) Take any action authorized by the Administrative Framework.

7.3. **Preventative Actions**. The Registry may also take preventative measures at its sole discretion, including any or all of the following:

(a) DNSSEC deployment which reduces the opportunity for pharming and other man-in-the-middle attacks;

(b) Removal of orphan glue records; and

(c) Place upon registry lock, hold or similar status a domain name during resolution of a dispute.

8. Transfer of Domain Names

A Registrant may not transfer a Domain Name, or an application for a Domain Name, without the prior written consent of Registry.