SCHEDULE A

dotCEO gTLD Policies

Document Description:

Effective Date: 20 January 2017	**Version:** 1.8
Approval Date:	**Contact:** Financial Controller

Document Control:

Date	Description	Modified
23 October 2014	**v1.2**	Christopher Murphy (General Manager – Legal and Finance)
20 January 2017	**v1.8**	Cameron Bale

Overview

The following policies, which govern the top level domain .CEO ("TLD" or "Registry) are based on policies and best practices drawn from Internet Corporation for Assigned Names and Numbers ("ICANN"), World Intellectual Property Organisation ("WIPO"), and other relevant sources, and is written to be consistent with ICANN Consensus Policies.

Specifically, the Registry Policies include the following interrelated policies, terms, and conditions (together the "Registry Policies"):

a. This **Overview**, including **Definitions**.

b. The **Naming Policy**, which describes reserved and blocked (prohibited) domain names;

c. The **Acceptable Use Policy** (AUP), which describes the types of acceptable uses for domain name registrations;

d. The **Privacy & Whois Policy**, which describes how a Registrant's Personal Information may be used by the Registry and in some cases, third parties;

e. The **Complaint Resolution Service** (CRS), which provides for the Registry, in cooperation with the Registrar, to provide a mechanism for Registrants and complainants to settle disputes concerning domain name registrations and/or uses; the CRS is a formal mediation-based dispute resolution process that provides a low-cost, efficient, neutral mechanism for fair adjudication of complaints including those from the public concerning alleged intellectual property abuses, illegal content, abusive or disruptive use of a domain name (e.g., phishing or spam) or other inappropriate conduct in the TLD; the CRS is complementary to the ICANN-mandated URS and UDRP.

The Registry policies form a cohesive framework and must be read in conjunction with one another, as well as with other applicable agreements, policies, laws, and regulations which, taken together, represent the entirety of the obligations and responsibilities with regard to any domain name registration.

Background

The Registry Polices are designed to promote transparent and non-discriminatory rules for the registration of domain names within this TLD, including fair and competitive pricing and competition at the Registrar level; protection of Registrant data and privacy; adherence by Registrants to the AUP; protection of intellectual property rights; protection of certain terms; prevention of the registration of illegal terms; prevention of violations of the law or abuse of the Domain Name System (DNS), including criminal acts; and to align use of the TLD with the applicable self-regulatory environment.

These polices provide that the TLD may, when necessary, implement Registry-level “Registration suspensions” for AUP violations. The registration and use of a domain is subject at all times to the Registry Polices, which provide the means to address crime, prohibited content, intellectual property abuses and other issues of concern.

Definitions

Abuse Point of Contact: an agent of the Registry appointed to review complaints for compliance with these Policies.

Acceptable Use Policy (or AUP): a policy that describes the types of acceptable uses for domain name registrations.

Blocked Names: a list of domain names, appearing on a list of blocked names, which list is subject to additions and modifications from time to time, which are indefinitely unavailable for registration.

Complaint Resolution Service (or CRS): which provides for the Registry, in cooperation with the Registrar, a mechanism for Registrants and complainants to settle disputes concerning domain name registrations and/or uses; the CRS is a formal mediation-based dispute resolution process that provides a low-cost, efficient, neutral mechanism for fair adjudication of complaints including those from the public concerning alleged intellectual property abuses, illegal content, abusive or disruptive use of a domain name (e.g., phishing, spam or child pornography) or other inappropriate conduct in the TLD; the CRS is complementary to the ICANN-mandated URS and UDRP.

Complainant: a party who files a complaint using the CRS.

Complaint: the complaint filed by a Complainant using the CRS.

Critical Issue Suspension (or CIS): a modification of the DNS records temporarily disabling a domain name from resolving; it may be undertaken, in Registry's sole discretion, when specifically requested by a Complainant in a CRS complaint, and when such Complaint alleges disruptive use of a domain name (e.g., phishing, spam, or child pornography) or other inappropriate conduct.

Data Escrow: the process of keeping a copy of critical data, including Whois data, with an independent third party.

Domain Name: an identification string that represents an Internet Protocol resource, usually a server computer hosting a web site. Is to the left of the dot in a URL; in "internic.net", the domain name is "internic".

Domain Name System (or DNS): the system that helps people find their way around the Internet. Every computer on the Internet has a unique address, which is a string of numbers, called an "IP address" (IP stands for "Internet Protocol"). Because IP addresses are hard to remember, the DNS makes using the Internet easier to navigate by allowing a familiar string of letters (the domain name) to be used instead of the IP address; so instead of typing 192.0.43.9, Internet users can type www.internic.net.

Domain Lock: a status code that can be set on a domain name in order to prevent unauthorized, unwanted or accidental changes to the domain name's ownership or technical information. When set, the following actions are prohibited: (i) modification of the domain name, including transferring the domain name; (ii) deletion of the domain name; and (iii) modification of the domain name contact details. Where a Domain Lock is applied, renewal of the domain name is still possible.

EPP (Extensible Provisioning Protocol): an industry standard for how Registrars communicate with Registries.

Escrow Agent: a third party contracted to perform data escrow services for the Registry.

ICANN (the Internet Corporation of Assigned Names and Numbers): the organization that creates the rules for, and ensures the technical stability of, the Internet.

ICANN Consensus Policies: domain name–related policies created through ICANN's multi–stakeholder consensus–based consultation process to govern certain actions related to domain names, Whois, and other ICANN-related functions; the current list of ICANN consensus polices can be found here.

Identical Match: means that a domain name consists of the complete and identical textual elements of a Trademark Clearinghouse–validated trademark. In this regard: (a) spaces contained within a mark that are either replaced by hyphens (and vice versa, as the context allows) or omitted; (b) only certain special characters contained within a trademark are spelled out with appropriate words describing it ("@" and "&"); (c) punctuation or special characters contained within a mark that are unable to be used in a second level domain name may either be (i) omitted or (ii) replaced by spaces, hyphens or underscores and still be considered Identical matches; and (d) no plural and no "marks contained" (i.e., "brandx" in "brandxproducts") qualify for inclusion.

Identifier: a number assigned by the Registry to a Registrant to uniquely identify the Registrant for the purposes of the Registry's operations and to preserve the Registrant's privacy; an individual's name is not used as an Identifier.

IP (Internet Protocol): the technical protocol that allows computers to find and communicate with each other on the Internet.

IP Address: a numerical address for a computer connected to the Internet.

Naming Policy: the policy that describes reserved and blocked (prohibited) domain names.

Name Server: the server that maps the domain name to an IP address.

Ombudsperson: an independent third party appointed by the Registry to identify and provide a neutral assessment of the interests of participants in the Complaint Resolution Service. In appropriate situations, may act as a mediator.

Personal Information: means information about an individual person, including any Registrant, whose identity can reasonably be ascertained from such information, but does not include indexes or aggregations of Personal Information relating to more than one person, such as logfiles, DNS Zone Files, databases or backups. This information may include the name, address, telephone number, and email address of the Registrant. This may include the home address and personal email of the Registrant, if the Registrant uses those as their primary contact information for the domain name.

Primary Purpose: the reasons for the Registry's collection of Personal Information, which is the storage and maintenance of such information in the Whois database (a copy of which ICANN requires is provided to the Escrow Agent) as required by ICANN, which is searchable and publicly available.

Privacy & Whois Policy: a policy document that describes how a Registrant's Personal Information may be used by the Registry and in some cases, third parties.

Prohibited Use: a use of the domain name that is illegal or expressly prohibited by the Policies, especially the Acceptable Use Policy.

Registered Domain Name: A Second Level Domain that has already being purchased by a third party.

Registrant: a person, whether an individual or business entity, in whose name a domain name is registered.

Registrant Agreement: the terms which Registrants must acknowledge and agree to in order to register a domain name; the Registrant Agreement binds Registrants, at the time of initial registration, domain renewal, or domain transfer, to the Registry Policies (which also includes by reference, ICANN-mandated rights protection mechanisms such as the Uniform Rapid Suspension service ("URS"), Uniform Domain Name Dispute Resolution Policy ("UDRP"), and other ICANN Consensus Policies);

Registrar: an entity, accredited by ICANN and under contract with the Registry, through which a business entity or individual may register a domain name.

Registrar Registration Fee: payment by the Registrar to the Registry for registration of a domain name.

Registration Fee: payment by the Registrant to the Registrar for registration of a domain name.

Registry: a database of all domain names and the associated registrant information in the top level domain; the entity that operates the TLD Registry database.

Registry Policies: the policy framework governing domain name registrations in the TLD, which includes the Naming Policy, Acceptable Use Policy, Registrant Agreement, Privacy & Whois Policy, Complaint Resolution Service, Registry–Registrar Agreement, ICANN consensus polices, and applicable laws, as amended from time to time.

Registry Related Parties: any natural or juristic person who is or is related to the Registry or the Registrar, including the officers, directors, shareholders, owners, managers, employees, agents, representatives, contractors, affiliates, successors, assigns, and attorneys of either the Registry or a Registrar.

Registry-Registrar Agreement (or RRA): the agreement between the Registry and each ICANN-

accredited Registrar which is authorized to sell domain names within the TLD.

Reserved Names: domain names currently unavailable for registration but which may be released in the future.

Respondent: the party against whom a CRS Complaint is filed; usually a Registrant.

Response: the reply by the Respondent in a CRS to the Complaint.

Root Servers: the authoritative name servers that serve the DNS root zone; a network of hundreds of servers in many countries around the world.

Sunrise: the exclusive period in which trademark owners may register the Identical Match of their trademark as a domain name prior to general domain name availability in the TLD.

Term: the period of registration of a domain name. The initial Term may be between one (1) and ten (10) years, but registration renewals may extend the Term.

Top Level Domain (or TLD): anything to the right of the final dot in a domain name; e.g., ".com", ".net", ".ie".

Trademark Claims Service: the service which gives notice to a prospective domain name registrant at the time of registration that the desired domain name may infringe a trademark; also provides electronic notice to a trademark rights holder that a domain name is an Identical Match to their trademark or to a previously-adjudicated infringing string has been registered. The prospective Registrant must warrant that: (i) they have received notification that the mark is registered in the Trademark Clearinghouse; (ii) they have received and understood the notice; and (iii) to the best of their knowledge, the registration and use of the requested domain name will not infringe on the rights that are the subject of the notice. If the domain name is registered subsequent to the notice being issued and the registrant attesting to its non–infringement, the registrar (through an interface with the Clearinghouse) will notify the mark holder(s) of the registration.

Trademark Clearinghouse (TMCH): the central storage repository of validated (authenticated) trademark rights–related data and information for dissemination with respect to trademark rights protection mechanisms and other registry-related services; more information can be found at their website.

Unassigned Domain Name: A Second Level Domain, reserved name or blocked name that has not yet been sold to a third-party, and which is retained by the Registry until sold.

UDRP (Uniform Domain Name Dispute Resolution Policy): an ICANN Consensus Policy that provides for independent adjudication of trademark-related domain name disputes concerning alleged trademark abuse.

URS (Uniform Rapid Suspension): similar to the UDRP, a complimentary rights protection mechanism that offers a lower-cost, faster path to relief for rights holders experiencing the most clear-cut cases of infringement.

Shared Registry System (SRS): the system that allows multiple Registrars to register domain names in a Registry.

Whois: an ICANN-mandated tool that displays the Registrant, Name Server, expiration date, and contact information for a domain name. Whois information is public and searchable, and may include Personal Information, including but not limited to:

a. Technical information on the DNS Name Servers resolving a domain name;
b. The date the domain name was inserted into the Registry's database;
c. The date of last modification;
d. The date of expiration;
e. The current status of the domain name;
f. The Registrar's contact details;
g. The Registrant's name;
h. The Registrant's physical address and/or alternate address;
i. The Registrant's email and phone numbers and/or alternate address;
j. The Registrant's state and/or alternate address;
k. The Registrant's country and/or alternate address.
l. Details of nominated administrative, technical and billing contacts.

WIPO: the World Intellectual Property Organization, an international body responsible for the promotion of the protection of intellectual property throughout the world and historic partner with ICANN for UDRP proceedings.

Zone File: the file on a Root Server that contains the domain name registration information necessary to resolve the domain names to their relevant IP addresses.

This Naming Policy sets forth the rules and guidelines concerning the availability of any domain name registered in this TLD. Here are the most current version of this Naming Policy and related material, including lists of Reserved Names, Blocked Names, and names that are blocked by ICANN. Certain other reserved and blocked names are provided exclusively to accredited Registrars.

This Naming Policy is part of the Registry Policies, which form a cohesive framework and must be read in conjunction with one another, as well as with other applicable agreements, policies, laws, and regulations which, taken together, represent the entirety the obligations and responsibilities with regard to any domain name registration.

Actual or attempted registration of a domain name in contravention of this Naming Policy may result in a Registrant being forbidden from registering domain names and/or the suspension or revocation of such Registrant's right to continue to be recognized as the Registrant of the non-compliant domain name or any other domain name. Suspension or revocation may, as determined in the Registry's sole discretion, with the cooperation of the sponsoring Registrar, apply to one or more of the Registrant's domain names.

The Registry reserves the right to modify or update this Naming Policy at any time and from time to time, and any such modifications or updates shall be posted on the Registry website. Once

posted, such modified or updated Naming Policy shall apply to all Registrants.

1. Reserved Names. Reserved names may be reserved by ICANN or the Registry.

    a. Reserved Names:

        i. ICANN Reserved Names:

            A. IGO/NGO Names

            B. Country Codes

        ii. Names Reserved by the Registry:

            A. Some domain names are reserved by the Registry for use in its operations. Refer to the appropriate Schedule A.

    b. In the event that a Registrant has been allowed to register a Reserved Name in violation of ICANN policy, the Registry will, in its sole discretion, with the cooperation of the sponsoring Registrar, cancel or transfer such domain name. Any fees paid by the Registrar to the Registry will be refunded but the Registrant and the Registrar shall have no further recourse under the Registry Policies or otherwise.

    c. In the event that a Registrant has fraudulently obtained the registration of a Reserved Name, the Registry reserves the right to cancel or transfer such domain name registration as provided for in, and take such further action as authorized by, the Registry Policies.

2. Blocked Names. The Registry reserves the right, in its sole discretion, to block certain names and terms from registration. The Registry may also block certain Domain Names in accordance with applicable law or ICANN Consensus Policies. Please refer to Schedule B for additional information regarding Blocked Names in the TLD.

    a. In the event the Registry has mistakenly allowed the registration of a Blocked Name, the Registry may, after refunding fees to the Registrar, transfer the name back to the blocked list.

3. Infringing Domain Names. Registrants are not allowed to register domain names which include terms that infringe upon intellectual property or other rights. More extensive discussions of infringement and the rights and responsibilities of both the rights holder and the alleged infringer can be found at ICANN's discussion of the UDRP, URS, and the TMCH claims service.

    a. Terms that may infringe upon the rights of others include, but are not limited to:

        i. company names, brand names, or product names;

        ii. sport team and association names;

iii. terms that may mislead the public as to a connection with or the source of goods or services, or the true identity of a person.

b. Registration or use of a domain name may be infringing if:

i. the domain name is identical or confusingly similar to a personal name, company, business, or other legal or trade name, or to a trade or service mark in which a third party has uncontested rights, including without limitation in circumstances which:

1) the registration or use is likely to deceive or confuse others in relation to the source of goods or services provided under or in relation to, or in respect of similar goods or closely-related services of a registered trademark; or

2) the registration or use deceives or confuses others in relation to the source of goods or services in respect of which an unregistered trademark or service mark has become a distinctive identifier of the goods or services of a third party complainant and in which the third party complainant has established a legal right; or

3) the registration or use trades on or passes off a domain name or a website or other content or services access through a resolution of a domain name as being the same as or endorsed by, authorised by, associated with, or affiliated with the established business, name, or reputation of another; or

4) the registration or use constitutes intentionally misleading or deceptive conduct in breach of the Registry Policies, applicable laws, or ICANN Consensus Policies; or

5) the domain name has been registered or used in bad faith, which includes, without limitation, the following:

A. the Registrant has registered or used the domain name primarily for the purpose of unlawfully disrupting the business or activities of another person or entity; or

B. by registering or using the domain name, the Registrant has intentionally created a likelihood of confusion with respect to the third party complainant's intellectual property rights or rights of publicity and as to the source, sponsorship, affiliation, or endorsement of website(s), email, or other online locations or services of a product or service available on or through resolution of the domain name.

c. The Registry does not reserve or block domain name registrations for terms, or confusingly similar terms, which might infringe upon intellectual property or other rights. It is the responsibility of the Registrant to determine, prior to registering a domain name, whether or not a term might infringe the intellectual property or other rights of an entity or individual.

The Registrant is solely liable in the event that the Registrants' use of a domain name constitutes an infringement or other violation of a third party's intellectual property or other rights.

d. In the event that any party disputes a Registrant's legal right to register and/or use a domain name that allegedly infringes the rights of another or that allegedly infringing material is displayed on a website which is resolved via the domain name, the Registrant shall act in accordance with and agrees to be bound by ICANN's policies, including the UDRP and URS, and by the Registry CRS, as applicable.

e. In the event that a Registrant has registered a domain name that infringes the rights of another, the Registry reserves the right, in cooperation with the sponsoring Registrar, to cancel or transfer such domain name registration as provided for in, and take such further action against Registrant as authorized by, these Registry Policies.

4. Two Letter/Two-Character Domains.

The registrant of a letter/letter two-character ASCII label must take steps to ensure against misrepresenting or falsely implying that the registrant or its business is affiliated with a government or country-code manager if such affiliation, sponsorship or endorsement does not exist.

5. Other Naming Policies.

a. Prospective Registrants are not permitted to submit an application for a domain name if they have previously submitted an application for registration for the same domain name where:

i. they are relying on the same eligibility criteria for each domain name applications; and

ii. the character string has previously been rejected by the Registry;

b. Registrants who repeatedly try to register Reserved Names, Blocked Names, or domain names that infringe the rights of others may be banned from further registration of domain names and may have any domain names registered to them revoked or cancelled, as provided for in the Registry Policies.

Schedule A

Info
Net
WWW
CEO
SLD
About
App
Apps
Contact
ContactUs
Domains
DomainName
DomainNames
DomainRegistrati
on
Home
Login
Love
Privacy
PrivacyPolicy
Social
SocialOS
Support
Terms
TOS
Wiki
AboutUs
CEO

Introduction

This Acceptable Use Policy (AUP) sets forth the terms and conditions for the use by a Registrant of any domain name registered in the top-level domain (TLD).

This Acceptable Use Policy (AUP) is part of the Registry Policies, which form a cohesive framework and must be read in conjunction with one another, as well as with other applicable agreements, policies, laws, and regulations which, taken together, represent the entirety the obligations and responsibilities with regard to any domain name registration.

The current version of the AUP will made available on the Registry website. It applies to any domain name registered in the TLD, no matter when or how registered, renewed, or transferred. Where a Registrant licenses or leases the domain name or any sub-domain names obtained under these Registry Policies, the Registry and the sponsoring Registrar shall hold the Registrant solely liable for activity in the domain name and in any sub-domain, if applicable.

The Registry supports the free flow of information and ideas over the Internet. The Registry does not and cannot exercise editorial control over the content of any message or web site made accessible by domain name resolution services in the TLD.

The Registry, with the cooperation of the sponsoring Registrar, may suspend, revoke, transfer, or modify the information or services provided in relation to any domain name (for example, through modification of a Registry Zone File) to address alleged violations of this AUP (described further below). The Registry shall have the authority to determine, in its sole discretion, whether use of a domain name is a *prima facie* violation of this AUP**.** The Registry or affected third parties may also utilize ICANN-sanctioned procedures, such as the Uniform Domain Name Dispute Resolution Policy (UDRP) or the Uniform Rapid Suspension (URS) system and/or applicable courts including those in the jurisdiction and venue specified in the Registrant Agreement.

Registrants are obliged and required to ensure that their use of a domain name is at all times lawful and in accordance with the requirements of the Registry Polices and applicable laws and regulations, including those of the Registrant's country of residence and ICANN Consensus Policies, including but not limited to 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 disclosures. Registrants who collect and maintain sensitive health and financial data must implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law. Where applicable, Registrants represent that they possesses any necessary authorisations, charters, licenses and/or other related credentials for participation in the sector associated with the TLD; material changes to the validity of such credentials must be reported to the Registry.

The Registry reserves the right to modify or amend this AUP at any time and from time to time and any such updates shall be posted on the Registry's website from time to time**.** The Registry will notify Registrars in the event of updates. The AUP as posted on the Registry's website is the agreement in affect at any time.

Prohibited Use

A Prohibited Use of a domain name is a use which is either illegal or expressly prohibited by provisions of this AUP and/or Registry Policies. A non-exhaustive list of such restrictions pertaining to registration or use of a domain name (in relation to various purposes and activities) is further described below in this AUP.

Compliance with the Registry's AUP

The registration and use of a domain name in the TLD must be for lawful purposes. The creation, transmission, distribution, storage of, or automatic forwarding to or framing of any material in violation of applicable laws, regulations, or this AUP is prohibited. This may include, but is not limited to, the following:

a. Communication, publication, or distribution of material (including through forwarding or framing) that infringes the intellectual property rights and/or right of publicity of another person or entity. Intellectual property rights include, but are not limited to copyrights, design rights, patents, patent applications, trademarks, rights of personality, and trade secret information. Rights of publicity include, but are not limited to, the right to keep one's image and likeness from being commercially exploited without permission or contractual compensation, the right to be left alone, and the right to be forgotten.

b. Cyber bullying or other harassment.

c. Registration or use of a domain name which, in the sole discretion of the Registry violates the Naming Policy.

d. Registration or use of a domain name which is part of a pattern of registration or use where the Registrant has registered or used domain names which violate the Naming Policy;

e. Failure of the Registrant to transfer the domain name to a third party if, as evidenced in writing, Registrant acted as an agent of the third party when registering for the domain name.

f. Use of content or methods which, in the sole discretion of the Registry:

    i. are capable of disruption of systems in use by other Internet users or service providers (*e.g.*, viruses or malware);

    ii. seek or apparently seek authentication or login details used by operators of other Internet sites (*e.g.*, phishing); or

    iii. may mislead or deceive visitors to the site that the site has an affiliation with the operator of another Internet site or business (*e.g.*, phishing).

g. Use of the domain name to publish or distribute, either directly or through forwarding or framing, images or materials that are prohibited by or constitute an offense under applicable

laws, including the law of the Registrant's country of residence.

h. Use of the domain name to publish or distribute material that includes, by way of example and without limitation, real or manipulated images depicting the sexual exploitation of children, bestiality, and material containing threats or detailed instructions regarding how to commit a crime.

i. Use of the domain name to publish or distribute defamatory material or material that constitutes racial vilification or “hate speech.”

j. Use of the domain name to publish or distribute material that constitutes an illegal threat or encourages conduct that may constitute a criminal act.

k. Use of the domain name to impersonate, mimic, defame or ridicule others.

l. Obtain a domain name that could be used to impersonate or mimic others.

m. Use of the domain name to publish or distribute material that is in contempt an order of a court or other authoritative government actor within the jurisdiction of the country of residence of the Registrant, Registrar, or Registry.

1. Electronic Mail

The Registry expressly prohibits Registrants from engaging in the following activities:

a. Communicating, transmitting, or sending unsolicited bulk email messages or other electronic communications (“junk mail” or “spam”) of any kind including, but not limited to, unsolicited commercial advertising and informational announcements as prohibited by applicable law.

b. Communicating, transmitting, or sending any material by email or otherwise that harasses another person or that threatens or encourages bodily harm or destruction of property.

c. Communicating, transmitting, sending, creating, or forwarding fraudulent offers.

d. Adding, removing, modifying, or forging any network header information with the effect of misleading or deceiving another person or attempting to impersonate another person by using forged headers or other forged identifying information (i.e., spoofing).

2. Disruption of the Registry Network

A Registrant may not use a domain name for the purpose of:

a. Restricting or inhibiting any person in their use or enjoyment of the Registry’s network or a domain name or any service or product of the Registry.

b. Actually or purportedly reselling the Registry’s services or products without the prior written

consent of the Registry.

c. Communicating, transmitting, or sending very large or numerous pieces of email or illegitimate service requests (i.e., a DDoS attack).

d. Providing false or misleading information to the Registry.

e. Facilitating or aiding the transmission of confidential information, private, personal or stolen data including, but not limited to, credit card information (without the owner's or cardholder's express written consent).

3. Network Integrity and Security

a. Registrants are prohibited from circumventing or attempting to circumvent the security of any host, network, or accounts (i.e., cracking or hacking) on, related to, or accessed through the Registry's network. This includes, but is not limited to:

   i. accessing data not intended for the Registrant;

   ii. logging into a server or account which the Registrant is not expressly authorised to access;

   iii. using, attempting to use, or attempting to ascertain a username or password without the express written consent of the operator of the service in relation to which the username or password is intended to function;

   iv. probing the security of other networks; and/or

   v. executing any form of network monitoring which is likely to intercept data, of any nature, not intended for the Registrant.

b. Registrants are prohibited from effecting any network security breach or disruption of any Internet communications including, but not limited to:

   i. accessing data of which the Registrant is not an intended recipient; and/or

   ii. logging onto a server or account which the Registrant is not expressly authorised to access.

   For the purposes of this section, "disruption" includes, but is not limited to:

   + port scans, TCP/UDP floods, packet spoofing;

   + forged routing information;

   + deliberate attempts to overload or disrupt a service or host; and/or,

+ using the Registry's network in connection with the use of any program, script, command, or sending messages with the intention or likelihood of interfering with another user's terminal session by any means, locally or by the Internet.

c. Registrants who compromise or disrupt the Registry's network systems or security may incur criminal or civil liability. The Registry will investigate any such incidents and will notify and cooperate with law enforcement and other appropriate governmental actors if an alleged crime or other alleged wrongdoing in violation of this AUP is suspected to have taken place.

4. Two-Letter/Two Character ASCII Labels

The registrant of a letter/letter two-character ASCII label must take steps to ensure against misrepresenting or falsely implying that the registrant or its business is affiliated with a government or country-code manager if such affiliation, sponsorship or endorsement does not exist.

5. Non-Exclusive, Non-Exhaustive

This AUP is intended to provide guidance as to acceptable use of the Registry's network and domain names. However, the AUP is neither exhaustive nor exclusive.

6. Enforcement

The Registry may, in its sole discretion, with the cooperation of the sponsoring Registrar, suspend, transfer, or terminate a Registrant's service, including a domain name registration, for violation of any of the terms and conditions of the AUP on receipt of a complaint if the Registry, in its sole discretion, believes:

a. a violation of the AUP has or may have occurred; and/or

b. suspension and/or termination may be in the public interest.

Except in extreme situations, the Registry may work with Registrars to effect the appropriate action. Notwithstanding the above, this AUP does not create any obligation on the part of the Registry to suspend, transfer, or terminate a Registrant's service for violations of this AUP, and Registry shall not be liable to any party for not enforcing the terms of this AUP.

7. DISCLAIMER AND LIMITATION OF LIABILITY

THE REGISTRANT ACKNOWLEDGES AND AGREES THAT, TO THE MAXIMUM EXTENT PERMITTED BY LAW, THE REGISTRY AND THE REGISTRY RELATED PARTIES SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF PROGRAMS OR OTHER DATA, OR OTHERWISE RELATING TO THE USE, SUSPENSION, TERMINATION OR THE INABILITY TO USE THE DOMAIN NAME OR IN ANY OTHER WAY RELATED TO THE DOMAIN NAME, REGARDLESS OF THE FORM OF ACTION, WHETHER IN

CONTRACT, TORT (INCLUDING IN THE CASE OF NEGLIGENCE BY THE REGISTRY AND/OR REGISTRY RELATED PARTIES), OR OTHERWISE. THE REGISTRY'S LIABILITY FOR ANY BREACH OF A CONDITION OR WARRANTY IMPLIED BY ANY OF THE REGISTRY POLICIES, INCLUDING THE NAMING POLICY, ACCEPTABLE USE POLICY, REGISTRANT AGREEMENT, PRIVACY & WHOIS POLICY, COMPLAINT RESOLUTION SERVICE, AND/OR THE REGISTRY–REGISTRAR AGREEMENT SHALL BE LIMITED TO THE MAXIMUM EXTENT POSSIBLE TO ONE OF THE FOLLOWING (AS THE REGISTRY MAY DETERMINE IN ITS SOLE DISCRETION:

A. SUPPLYING THE DOMAIN NAME AGAIN; OR

B. PAYING THE REASONABLE COST INCURRED OF HAVING THE SERVICES SUPPLIED AGAIN.

ADDITIONALLY, TO THE MAXIMUM EXTENT PERMITTED BY LAW, THE REGISTRY AND THE REGISTRY RELATED PARTIES SHALL NOT BE LIABLE FOR ANY LOSSES OR DAMAGES THAT THE REGISTRANT MAY INCUR AS A RESULT OF UNAUTHORIZED USE OF THE DOMAIN ARISING FROM "HACKING," DENIAL OF SERVICE ATTACK, VIRUS, WORM, OR OTHERWISE, OR FOR LACK OF FITNESS FOR A PARTICULAR PURPOSE OF THE DOMAIN NAME OR SERVICES RELATED TO THE DOMAIN NAME.

IN THE EVENT THAT THE REGISTRY OR A REGISTRY RELATED PARTY TAKES ACTION WITH RESPECT TO A REGISTRY DOMAIN NAME PURSUANT TO THE REGISTRY POLICIES, WHICH ACTION IS REVERSED, MODIFIED, OR ACKNOWLEDGED TO HAVE BEEN INCORRECT BY THE REGISTRY AND/OR A REGISTRY RELATED PARTY, BY OR THROUGH THE REGISTRY COMPLAINT RESOLUTION SERVICE, OR BY A COURT, THEN REGISTRANT AGREES THAT, TO THE MAXIMUM EXTENT PERMITTED BY LAW, THE REGISTRY AND/OR REGISTRY RELATED PARTIES SHALL NOT BE LIABLE FOR ANY DAMAGES THAT THE REGISTRANT MAY SUFFER THEREBY, EVEN IF THE REGISTRY AND/OR REGISTRY RELATED PARTIES HAVE BEEN ADVISED OF THE POTENTIAL FOR SUCH DAMAGES, AND EVEN IF THE REGISTRY AND/OR REGISTRY RELATED PARTIES MAY FORESEE SUCH POSSIBLE DAMAGES. THE REGISTRANT'S SOLE REMEDY UNDER SUCH CIRCUMSTANCES SHALL BE THE RESUPPLY OF THE DOMAIN NAME OR, AT THE SOLE DISCRETION OF THE REGISTRY, A REFUND OF THE REGISTRATION FEE, RENEWAL FEE (IF THE CIRCUMSTANCE OCCURRED DURING A RENEWAL TERM) OR REDEMPTION FEE, WHICH REMEDY THE REGISTRANT AGREES CONSTITUTES THE ONLY POSSIBLE DIRECT DAMAGES FLOWING FROM THIS AGREEMENT.

IN ADDITION, THE REGISTRY AND/OR REGISTRY RELATED PARTIES ARE, TO THE MAXIMUM EXTENT PERMITTED BY LAW, NOT LIABLE FOR ANY DAMAGES THAT THE REGISTRANT MAY SUFFER BECAUSE OF SERVICE OR SYSTEM FAILURE, INCLUDING DOMAIN NAME SYSTEM FAILURE, ROOT SERVER FAILURE, TELECOMMUNICATION FAILURE, INTERNET PROTOCOL ADDRESS FAILURE, ACCESS DELAYS OR INTERRUPTIONS, DATA NON-DELIVERY OR MIS-DELIVERY, ACTS OF GOD, UNAUTHORISED USE OF PASSWORDS, ERRORS, OMISSIONS OR MIS-STATEMENTS IN ANY INFORMATION OR OTHER SERVICES PROVIDED UNDER THIS AGREEMENT, DELAYS OR INTERRUPTIONS IN DEVELOPMENT OF WEB SITES, RE-DELEGATION OF THE REGISTRY TOP-LEVEL DOMAIN NAME, OR BREACH OF SECURITY, EVEN IF THE REGISTRY

AND/OR REGISTRY RELATED PARTIES HAVE BEEN ADVISED OF THE POTENTIAL FOR SUCH DAMAGES, AND EVEN IF THE REGISTRY OR REGISTRY RELATED PARTIES MAY FORESEE SUCH POSSIBLE DAMAGES. THE REGISTRANT'S SOLE REMEDY FOR THE REGISTRY OR REGISTRY RELATED PARTIES' BREACH OF THIS AGREEMENT OR NEGLIGENCE OF ANY TIME SHALL BE, AT THE SOLE DISCRETION OF THE REGISTRY OR THE REGISTRY RELATED PARTIES, THE RESUPPLY OF THE DOMAIN NAME OR A REFUND OF THE REGISTRATION FEE, REDEMPTION FEE OR RENEWAL FEE (IF THE BREACH OCCURS DURING A RENEWAL TERM), WHICH REMEDY THE REGISTRANT AGREES CONSTITUTES THE ONLY POSSIBLE DIRECT DAMAGES FLOWING FROM THIS AGREEMENT. THE REGISTRANT'S SOLE REMEDY FOR AN ACTION NOT FLOWING FROM THIS AGREEMENT (IN TORT OR OTHERWISE) SHALL BE LIMITED TO THE AMOUNT OF MONEY PAID TO THE REGISTRY OR REGISTRY RELATED PARTIES BY THE REGISTRANT.

8. Modification of Network Data

The Registry is committed to an open Internet and to freedom of expression. However, in the course of its duties to comply with ICANN consensus policies, UDRP, URS, or CRS decisions, court or other governmental orders, or other duly-qualified law enforcement requests, or to protect the integrity and functioning of its networks, the Registry, in its sole discretion, reserves the right to:

a. remove or alter content, Zone File data and/or other material from its servers that violates the provisions or requirements of this AUP;

b. re-delegate, redirect or otherwise divert traffic intended for any service;

c. notify operators of Internet security monitoring services, virus scanning services and/or law enforcement authorities of any breach or apparent breach of this AUP or other Registry Policies; and/or

d. terminate access to the Registry's network by any person or entity that the Registry determines has violated the provisions or requirements of this AUP.

1. Preamble

This Privacy & Whois Policy is part of the Registry Policies, which form a cohesive framework and must be read in conjunction with one another, as well as with other applicable agreements, policies, laws, and regulations which, taken together, represent the entirety the obligations and responsibilities with regard to any domain name registration.

2. Objectives

The objectives of this Privacy & Whois Policy are:

a. To disclose to the Registrant, and in doing so obtain the Registrant's consent to, the fact that certain Personal Information provided by the Registrant may be dealt with in the following manner by the Registry:

   i. Personal Information shall be collected and may be used, maintained, and/or corrected from time to time in accordance with this and/or other Registry Policies or practices;

   ii. Personal Information shall be collected by the Registry through the Registrar for the purpose of the storage, maintenance, disclosure, and/or use of such Personal Information. The Registry may disclose or transfer such Personal Information to any third party (in addition to ICANN and the Registry Escrow Agent), under the circumstances detailed in the "Use and Disclosure" section of this Privacy & Whois Policy;

   iii. All Personal Information about the Registrant which is supplied to the Registry, or a Registrar, may be available to third parties by way of a public "Whois" service, consistent with:

      1) Privacy principals of the Registry;

      2) The Registry Policies;

      3) ICANN Consensus Policies; and/or

      4) Applicable laws, rules and regulations.

b. To outline the Registry's procedures for the appropriate collection, holding, use, correction, disclosure, and transfer of a Registrant's Personal Information by the Registry.

In order to provide Registry services in any TLD, the Registry is required by ICANN to collect and publish data pertaining to the identity of the Registrant of any domain name.

3. Definitions

In addition to definitions found in the Registry Policies "Policy Overview and Definitions" document, the following terms are used in this Privacy & Whois Policy as defined below.

a. "Escrow Agent" means a third party contracted to perform data escrow services for the Registry. The data escrow agreement with the Escrow Agent ensures the transfer of all relevant DNS data and Registrant information, including Personal Information, to ICANN and an ICANN-mandated back-up registry operator ("EBERO" or Emergency Back End Registry Operator), and will ensure the safety and integrity of the Registry's TLD database. The Escrow Agent is prohibited from use or disclosure of the Registry's TLD data unless that use or disclosure is deemed essential to ensure the stability and integrity of the Registry's TLD.

b. "Personal Information" means information about an individual person, including any Registrant, whose identity can reasonably be ascertained from such information, but does not include indexes or aggregations of Personal Information relating to more than one person, such as logfiles, DNS Zone Files, databases or backups. This information may include the name, address, telephone number, and email address of the Registrant. This may include the home address and personal email of the Registrant, if the Registrant uses those as their primary contact information for the domain name.

c. The "Primary Purpose" of the collection of Personal Information is the storage and maintenance of such information in the Whois database (a copy of which ICANN requires is provided to the Escrow Agent) as required by ICANN, which is searchable and publicly available. No domain name can be registered without the Registry collecting such Personal Information and making it publicly available in the Whois database.

4. "Whois" Server Implications

The Registry will maintain a publicly accessible information service known as the Registry's "Whois" service, which service provides the following information pertaining to a domain name, pursuant to ICANN's Consensus Policies, which may be amended at any time and from time to time:

a. Technical information on the DNS servers resolving a domain name;

b. The date the domain name was inserted into the Registry's database;

c. The date of last modification;

d. The date of expiration;

e. The current status of the domain name;

f. The Registrar's contact details;

g. The Registrant's name;

h. The Registrant's physical address and/or alternate address;

i. The Registrant's email and phone numbers and/or alternate address;

j. The Registrant's state and/or alternate address;

k. The Registrant's country and/or alternate address.

l. Details of nominated administrative, technical and billing contacts.

It is not possible to entirely block third party access to Registrant Personal Information; it may however, be possible for Registrants to use the services of a third party to display "private" or "proxy" information in the publicly-available Whois.

5. Collection

a. The Registry collects Personal Information for one or more of its functions and/or activities including, where required:

   i. to identify and maintain contact details of domain name Registrants and their duly appointed agents;

   ii. to provide access to that data to the public and persons connected with Registrants;

   iii. to provide services to Registrants and maintain its database;

   iv. for the provision of Whois service;

   v. to contact the Registrant, including notifications in accordance with the Registry Polices; and/or,

   vi. to provide law enforcement, government agencies, and relevant Internet security organisations with information required to investigate or prevent an alleged crime.

b. The Registry's website utilizes technology that collects user information and tracks usage (e.g., via "cookies"). The Registry's website may feature links to other third party websites but the Registry is not responsible for the content and privacy practices of any such third party websites.

6. Use and Disclosure

a. The Registry may use or disclose Personal Information about a Registrant for a purpose other than the Primary Purpose of collection where:

   i. The Personal Information consists of the contact details of a person connected to a Registrar, Internet service provider, Internet service reseller, or persons connected thereto, such as directors, managers or other points of contact;

   ii. The Registrant has consented to such use or disclosure; or

iii. The Registry believes in its sole judgment that the use or disclosure is necessary:

1) To lessen or prevent a serious and imminent threat to an individual's life, health, or safety; or

2) To lessen or prevent a serious threat to public health or public safety; or

3) Because the Registry has reason to suspect that unlawful activity or a violation of the any of the Registry's Policies has been, is being, or may be engaged in, and uses or discloses the Personal Information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons (including parties affected by that violation) or authorities; or

4) Because the use or disclosure is required or authorised by or under law, rule or regulation; or

5) Because the Registry believes that the use or disclosure is necessary for one or more of the following, by or on behalf of an enforcement body:

a) The prevention, detection, investigation, prosecution, or punishment of criminal offences, breaches of a law imposing a penalty or sanction, or breaches of a prescribed law;

b) The preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; or

6) As ordered by a dispute resolution provider in connection with a Uniform Domain Name Dispute Resolution Policy (UDRP) or Universal Rapid Suspension (URS) proceeding, as mandated by ICANN.

7) As decided by parties resulting from a CRS dispute.

8) For any other legal purpose, excluding marketing.

b. Nothing in this Section 6 "Use and Disclosure" requires the Registry to disclose any Personal Information; the Registry is always entitled not to disclose Personal Information in the absence of a legal obligation to disclose it.

c. The Registry may also be subject to the requirements of present, and any future, policy dealing with cross-border data flows if it transfers Personal Information to a person or entity in a foreign country situated outside of the European Economic Association (EEA).

d. The Registry maintains and uses servers in diverse locations internationally, necessitating transfer of data, including Personal Information, between servers and data networks.

e. The Registry shall never use Personal Information of a Registered Name Holder, acquired under this agreement, to contact the Registered Name Holder with a communication

intended or designed to induce the Registered Name Holder to change Registrar's, or for the purpose of selling non-Registry services to the Registered Name Holder. Notwithstanding the foregoing, nothing in this Agreement shall prevent the Registry, or its related companies, from offering or selling products and services to Registered Name Holders who are known to the Registry though existing customer relationships, provided that Registry does not use Personal Information provided by the Registered Name Holder to trigger a process to target Registered Name Holders.

7. Data Security

a. The Registry shall take the steps required by ICANN, the laws of the Commonwealth of Australia, and any other applicable law to protect the Personal Information it holds from misuse and loss and from unauthorised access, modification or disclosure to the extent required by law.

8. Openness

a. This Privacy & Whois Policy sets out the Registry's policies concerning its management of Personal Information. The Registry shall make this document available to anyone who asks for it and on its website.

9. Access and Correction

a. If the Registry holds Personal Information about a Registrant, it shall provide that Registrant with access to such information upon receipt of written request by the Registrant, except to the extent that the Registry believes in its sole discretion:

   i. In the case of Personal Information, providing access may pose a serious and imminent threat to the life or health of any individual; or

   ii. Providing access may have an unreasonable impact upon the privacy of other individuals; or

   iii. The request for access is frivolous or vexatious; or

   iv. The information relates to existing or anticipated legal proceedings and the information would not be accessible by the process of discovery in those proceedings; or

   v. Providing access may be unlawful; or

   vi. Denying access may be required or authorised by or under law, rule or regulation, including, but not limited to, the order of any court having appropriate jurisdiction; or

   vii. Providing access may prejudice an investigation of possibly unlawful activity; or

   viii. Providing access may prejudice:

1) The prevention, detection, investigation, prosecution or punishment of criminal offences, or other breaches of law; or

2) The preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders; or

3) A law enforcement body or relevant Internet security organisation performing a lawful security function requests that the Registry not provide access to the information on the basis that providing access would be likely to cause harm.

b. The Registry shall not in any event be under any obligation to disclose DNS Zone Files, payment logs, email archives, or data backups to any party, except as required by ICANN, law, or court order.

c. Where providing access would reveal evaluative information generated within the Registry in connection with a commercially sensitive decision-making process, the Registry may give the Registrant an explanation for the commercially sensitive decision rather than access to the information.

d. If the Registry holds Personal Information about a Registrant and the Registrant is able to establish that the information is not accurate, complete, and up-to-date, upon notice of such fact from the Registrant, the Registry shall take reasonable steps to correct the information so that it is accurate, complete, and up-to-date as requested by the Registrant, except where the data is contained in an historical record or archive.

10. Review of Policy

The Registry reserves the right to review or revise this Privacy & Whois Policy at its sole discretion within one hundred eighty (180) days prior written notice, including to maintain compliance with ICANN Consensus Policy or other applicable law or regulation; Registrants who have provided their Personal Information to the Registry are deemed to acknowledge and be bound by this Privacy & Whois Policy and any changes made to it.

The current version of the Privacy & Whois Policy will made available on the Registry website. It applies to any domain name registered in the TLD, no matter when or how registered, renewed, or transferred. Where a Registrant licenses or leases the domain name or any sub-domain names obtained under these Registry Policies, the Registry and the sponsoring Registrar shall hold the Registrant solely liable for activity in the domain name and in any sub-domain, if applicable.

This Complaint Resolution Service (CRS) is part of the Registry Policies, which form a cohesive framework and must be read in conjunction with one another, as well as with other applicable agreements, policies, laws, and regulations which, taken together, represent the entirety the obligations and responsibilities with regard to any domain name registration.

Ordinarily, the Registry is unable to simply suspend a domain name where another member of the public complains or takes issue with the use to which a domain name is being put and a concerned member of the public always has the right to reach out to the domain name Registrant directly to bring any concerns to their attention.

If such direct contact is not possible or advisible (it may be a sensitive concern after all), or if after doing so, there is still a concern that the registration or use of a domain name in the TLD is illegal, abusive, infringes the rights of others, is otherwise in violation of the Registry Policies, or is allegedly otherwise in violation of the law, we provide the CRS, through which anyone may register a complaint.

The CRS provides a transparent, efficient, and cost effective way for the public, including law enforcement, regulatory bodies, and intellectual property owners to (a) submit complaints or report concerns regarding the registration or use of a domain name in the TLD, and (b) where appropriate, to seek to have such concerns addressed through confidential and non–binding mediation.

Managed through the Abuse Point of Contact and a corresponding webform, the CRS provides a procedure for reporting and, where appropriate, addressing alleged illegal or prohibited conduct effected through a domain name in the TLD; prohibited conduct includes, but is not limited to: inaccurate Registrant Whois information; that a domain name registration is being used to facilitate or promote malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting, or activity otherwise contrary to applicable law. The CRS framework employs two levels of review: (1) immediate action to protect the public interest, or (2) the optional appointment of an independent Ombudsperson to facilitate, where possible, confidential and non-binding complaint resolution between the parties.

The CRS is not intended to replace courts or ICANN-mandatory dispute resolution systems such as the UDRP (Uniform Domain Name Dispute Resolution Procedure) or URS (Uniform Rapid Suspension system).

To submit a complaint or report a concern regarding the registration or use of a domain name in the TLD, please use the CRS Complaint form.

Complaints and reports of concern will be reviewed as follows.

Step One: Confirmation and Communication

The Abuse Point of Contact will initially review all complaints and reports of concerns regarding alleged criminal or otherwise illegal or prohibited conduct for compliance with the Registry Policies.

Upon receipt of any Complaint, the Abuse Point of Contact will "lock" the domain name and associated records until the Complaint is determined frivolous, resolved, withdrawn, or dismissed, or pursuant to a court order or reasonable request from law enforcement. A Complaint shall not exceed 1,000 words or three (3) pages, whichever is less. Abuse Point of Contact will notify Registrar in the event a domain name has been locked.

Review Tier 1: immediate action to protect the public interest: In the event of a report of alleged criminal or otherwise illegal or prohibited conduct requiring immediate action to protect the public interest, the Abuse Point of Contact will initiate an "Immediate Review of Request for Suspension in the Public Interest" (see Step Two below).

Review Tier 2: optional appointment of an independent Ombudsperson: In the event of a Complaint alleging non-compliance with the Registry Policies that does not require immediate action to protect the public interest, the Abuse Point of Contact will contact the parties to explore their interest in confidential and non-binding mediation aimed at facilitating an amicable resolution between the parties (see Steps Three through Seven below).

If the Abuse Point of Contact considers that the Complaint does not address a matter covered by the Registry Policies, is deficient, or is frivolous, the filing/complaining party (Complainant) will be promptly notified of the deficiencies identified. The Complainant has five (5) business days from the receipt of notification to correct the deficiencies and return the Complaint, failing which, the Abuse Point of Contact will deem the Complaint to be withdrawn and the domain lock will be removed. This will not prevent the Complainant from submitting a different Complaint in the future.

Step Two: Immediate Review of Request for Suspension in the Public Interest

On receipt of a Complaint or report of alleged criminal or otherwise illegal or prohibited conduct requiring immediate action to protect the public interest, the Abuse Point of Contact will initiate an "Immediate Review of Request for Suspension in the Public Interest" to determine, whether or not specifically requested by the Complainant, if a Critical Issue Suspension (CIS) is warranted.

A request for a CIS may be granted in cases where there is a compelling and demonstrable threat to the stability of the Internet, critical infrastructure, or public safety. A CIS does not terminate the Registrant's rights or their domain name registration; it simply modifies the Name Server records in the zone, temporarily disabling resolution. Suspensions under the CRS, including a CIS, may be appealed to the Ombudsperson's office for resolution.

Absent compelling circumstances including, but not limited to, a court order or reasonable request from law enforcement, where the Abuse Point of Contact has activated a CIS, a suspension notice will be sent to the Registrant's administrative contact with a copy to the Registrar, usually within 48 hours.

Step Three: Formal Notification of Complaint

Any Complaint alleging non-compliance with the Registry Policies must be submitted to the Abuse Point of Contact using the webform provided on the Regsitry's website; all required fields must be complete, the Complaint must be signed electronically, and any fee required by the webform must be paid in advance of the Abuse Point of Contact attending to the complaint. The types of conduct that may be raised as the basis for a Complaint alleging non-compliance with the Acceptable Use Policy can be found on the Registry's website.

In the event that a Complaint alleging non-compliance with the Registry Policies is submitted to the Abuse Point of Contact, typically within 5 business days of receipt of the Complaint, the Abuse Point of Contact will send a "Formal Notification of Complaint" including a copy of the Complaint, by email to the Respondent using the administrative contact details provided in the Whois for the domain name as well as to any other Registrant email addresses provided by the Complainant.

Either Party may provide an additional email address by notifying the Abuse Point of Contact; the Registrant may not, however, change the Registrant information for the domain name without mutual agreement of the parties or unless a settlement is reached.

Communications must be in English and any email attachments should be in a standard format, such as Microsoft Word or PDF, and should not exceed 10MB individually or 50MB together.

Any communication between the Parties shall copy the other Party, the Abuse Point of Contact, and the Ombudsperson, if appointed.

Except as otherwise decided by the Abuse Point of Contact in its sole discretion, all communications under the CRS shall be deemed received at the date and time on which the email or communication was sent as determined by the time zone of the Abuse Point of Contact; in case of doubt, however, it shall be the responsibility of the sending party to provide proof of transmission.

Step Four: Commencement of Complaint Resolution Service Proceedings

At the same time as the notification to the Parties (by email) of the commencement of a CRS proceeding, the Abuse Point of Contact will contact the parties to explain the confidential and non-binding nature of the CRS, and to gauge their interest in Registry-facilitated mediation aimed at allowing the Parties to reach an amicable solution.

For the avoidance of doubt, even if the Parties do not decide to engage in CRS-based mediation, the Registry may, in its sole discretion (including based on reports made to the Registry by third parties), suspend, transfer, or terminate a Registrant's service, including a domain name registration, for violation of any of the requirements or provisions of the Registry Policies on receipt of a complaint if the Registry believes (a) a violation has or may have occurred; and/or (b) suspension and/or termination may be in the public interest. Also, for the avoidance of any doubt, the Respondent may submit a Response even if it decides not to participate in mediation, e.g., to provide information to the Registry as to any alleged non-compliance.

Step Five: the Response

Within fifteen (15) business days of the date of commencement of a CRS proceeding, the Respondent (i.e., the domain name Registrant) may submit a Response.

The Response must be submitted to the Abuse Point of Contact using the webform provided on the Registry's website; all required fields must be completed, and the Response must be signed electronically.

Using the Registry's webform, the Response shall:

a. **specifically dispute each alleged instance of non-compliance (the "grounds for the Complaint") raised by the Complainant that the Respondent wishes to rely upon to rebut the Complainant's assertions;**

b. **indicate whether the Respondent wishes to be contacted directly or through an authorized representative—if the Respondent wishes to use an authorized representative, their contact details including email address must be provided;**

c. **mention whether any legal proceedings have been commenced (even if terminated) in connection with the domain name(s) which is the subject of the Complaint; and**

d. **not exceed 1,000 words or three (3) pages, whichever is less.**

Once submitted, a copy of the Response will be forwarded to the Complainant and to the Respondent as soon as practicable. In the event there is no Response, the Complaint shall be deemed closed; the Parties may however submit a new Complaint in future, or a UDRP or URS or court claim.

Step Six: Reply by the Complainant

Within five (5) business days of receiving the Respondent's Response, the Complainant may submit a Reply to the Respondent's Response, which shall not exceed 1,000 words or three (3) pages, whichever is less (annexes may only be included with the permission of the Abuse Point of Contact). The Reply should be confined to answering any new points raised in the Response that could not have reasonably been foreseen when the Complaint was submitted.

Step Seven: Amicable Complaint Resolution (Ombudsperson)

If the Parties have agreed to mediation, within ten (10) business days of the receipt of the Complainant's Reply (or the expiry of the deadline to do so), the Abuse Point of Contact will arrange with the Ombudsperson's office for mediation to be conducted. Mediation will be conducted in a manner that the Ombudsperson, at their sole discretion, considers appropriate.

Mediation conducted between the Parties during mediation (including any information obtained from or in connection to negotiations) shall be strictly confidential as between the Parties and the Ombudsperson. Neither the Ombudsperson nor any Party may use or reveal details of such negotiations to any third parties (including a UDRP or URS provider) unless ordered to do so by a court of competent jurisdiction.

If the Parties reach settlement during the mediation, then the existence, nature, and terms of the settlement shall be confidential as between the Parties unless the Parties specifically agree otherwise, a court competent jurisdiction orders otherwise, or applicable laws or regulations require it.

Any settlement reached by the Parties must be in writing to be enforceable and should include instructions for the Registry (and if applicable, Registrar) concerning the disposition of domain name and timing; the Ombudsperson will provide a (non-mandatory) template for such purposes.

If the Parties did not achieve an acceptable resolution through mediation within twenty (20) business days of the appointment of an Ombudsperson, the Ombudsperson will send notice to the Parties and Abuse Point of Contact that it does not appear that the Complaint can be resolved through the CRS. In such case, the Complainant shall have the option of availing itself of the courts or other processes such as the UDRP or URS. The Registry shall unlock the domain name within fifteen (15) business days of such notice from the Ombudsperson.

Effect of Court Proceedings

If, before or during the course of proceedings under the CRS, the Ombudsperson or Abuse Point of Contact is made aware that legal proceedings have begun in or before a court or other body of competent jurisdiction, including but not limited to a URS or UDRP proceeding, and that such legal proceeding specifically relates to a domain name and conduct which is the subject of a Complaint, the CRS will be terminated.

A Party must promptly notify the Ombudsperson if it initiates or becomes aware of legal proceedings before a court or panel of competent jurisdiction, including but not limited to a URS or UDRP proceeding, relating to a domain name which is the subject of a Complaint during the course of proceedings under the CRS.

The applicable fees with respect to the referral of proceedings under the CRS to the Ombudsperson are (in AUD) $100 plus applicable taxes for Complaints involving 1-5 domain names and only one Complainant. For Complaints involving 6 or more domain names, the Ombudsperson and/or Abuse Point of Contact will set a fee in consultation with the Abuse Point of Contact. Fees are calculated on a cost-recovery basis; the Registry does not intend profit from its mediation or administration services of the Complaint Resolution Service.

Exclusion of Liability

Neither the Registry employees, directors, officers, representatives, delegees, shareholders, agents, successors, and/or assigns or those of its affiliates; nor any employee or agent of the Ombudsperson shall be liable to a Party for anything done or omitted, whether (to the extent permitted by applicable law) negligently or otherwise, in connection with any proceedings under the CRS unless the act or omission is shown to have been intentionally done in bad faith.