GAC Advice Response Form for Applicants

The Governmental Advisory Committee (GAC) has issued advice to the ICANN Board of Directors regarding New gTLD applications. Please see Section IV, Annex I, and Annex II of the GAC Beijing Communique for the full list of advice on individual strings, categories of strings, and strings that may warrant further GAC consideration.

Respondents should use this form to ensure their responses are appropriately tracked and routed to the ICANN Board for their consideration. Complete this form and submit it as an attachment to the ICANN Customer Service Center via your CSC Portal with the Subject, "[Application ID] Response to GAC Advice" (for example "1-111-11111 Response to GAC Advice"). All GAC Advice Responses must be received no later than 23:59:59 UTC on 10-May-2013.

Respondent:

Applicant Name	Tucows TLDs Inc.
Application ID	1-1171-56570
Applied for TLD (string)	.MEDIA

Response:

Tucows TLDs Inc. has received and considered the GAC's advice concerning applications for the .MEDIA gTLD, and welcomes the opportunity to respond.

About Tucows TLDs Inc. and .MEDIA

Tucows seeks to provide simple, useful services that help people unlock the power of the Internet. Our mission is to provide a web address and email address for every person and business.

We believe .MEDIA will provide Internet users with an easier means of recognizing web and email addresses featuring content or services related to the wide range of purposes the term 'media' provides. Moreover, .MEDIA will make additional memorable, relevant names available to new registrants. We believe less confusion provides a substantial benefit to the Internet user community, as it will allow them to more easily and more readily understand the purpose or motives of the registrant's website or email, allowing for better, more efficient and more effective use of their time online.

Addressing a perceived higher level of risk associated with consumer harm

We firmly believe that a strong abuse and security policy is key to a safe, successful gTLD. As part of our commitment to mitigate and minimize abusive registrations that have a negative impact on Internet users and rights holders, we made a number of assurances in both our initial application and our Public Interest Commitments, which we submitted for .MEDIA in February 2013. These 11 specific commitments included:

• Introducing a robust complaints handling process, and a commitment to timely review, resolve and respond to reported cases of abuse;
• Requiring registrars to adopt and enforce our Acceptable Use Policy (AUP) during the sales process, which includes a number of commitments and enforceable processes designed to ensure registered domain names will be used only for legitimate activities;
• Committing to provide an easily accessible flagging process to allow members of the public, law enforcement and other government entities to quickly and easily call attention to possible cases of non-compliance with our AUP.

GAC ADVICE: Safeguards applicable to all new gTLDs

Regarding safeguards the GAC believes should apply to all new gTLDs, we present the following responses:

1. WHOIS verification and checks — Registry operators will conduct checks on a statistically significant basis to identify registrations in its gTLD with deliberately false, inaccurate or incomplete WHOIS data at least twice a year. Registry operators will weight the sample towards registrars with the highest percentages of deliberately false, inaccurate or incomplete records in the previous checks. Registry operators will notify the relevant registrar of any inaccurate or incomplete records identified during the checks, triggering the registrar's obligation to solicit accurate and complete information from the registrant.

With registrar experience managing more than 14 million gTLDs and ccTLDs ingrained in the fabric of our corporate culture, WHOIS accuracy has always been of paramount of importance. As a result, we commit to conducting checks twice yearly to identify registrations with false, inaccurate or incomplete data. We further commit to notifying the relevant registrar of any accurate or incomplete records. Moreover, our Compliance Administrator and related team will be responsible for resolving issues in a timely fashion.

2. Mitigating abusive activity — Registry operators will ensure that terms of use for registrants include prohibitions against the distribution of malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law.

Our AUP, as described in section 29 of our application, defines a set of unacceptable behaviors by domain name registrants in relation to the use of their domain names. It specifically bans, among other practices, the use of a domain name for abusive or illegal activities, including spamming, phishing, willful distribution of malware, piracy, and the distribution of any other illegal material that violates the legal rights of others, including but not limited to rights of privacy or intellectual property protections.

We have always taken abusive activity extremely seriously within our registrar business, and pledge to continue to do so within our registry business.

3. Security checks — While respecting privacy and confidentiality, Registry operators will periodically conduct a technical analysis to assess whether domains in its gTLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. If Registry operator identifies security risks that pose an actual risk of harm, Registry operator will notify

the relevant registrar and, if the registrar does not take immediate action, suspend the domain name until the matter is resolved.

As outlined in section 28.2 of our application, we have committed to introducing a significant abuse mitigation and prevention program based on best practice policy recommendations developed by the Council of Country Code Administrators (CoCCA), on lessons learned from previous gTLD launches, on the operating experience of TLDs such as .COM, and on participation in policy working groups and debate at ICANN. The Program is comprised of policies, procedures and resource allocation that aim to prevent and mitigate abusive practices at all levels of registry operations and domain name use.

A total of 25 ccTLDs use the CoCCA policy framework to ensure protection of the registry, and to minimize abusive registrations and other activities that affect the legal rights of others. We have updated the best parts of these policies to the new gTLD environment to protect the specific needs of the registry and the registrants, and the rights and needs of third parties. Wherever applicable, we also follow the recommendations of NIST SP 800-83 Guide to Malware Incident Prevention and Handling.

The prevention aspect of this policy requires us to proactively monitor the .MEDIA zone and assess whether domains are being used to perpetrate security threats (including pharming, phishing, malware and botnets). We reserve the right in our AUP, and will not hesitate to use that right, to shut down or block services, such as email, that are used as vectors by malware producers or other sources of abuse.

4. Documentation — Registry operators will maintain statistical reports that provide the number of inaccurate WHOIS records or security threats identified and actions taken as a result of its periodic WHOIS and security checks. Registry operators will maintain these reports for the agreed contracted period and provide them to ICANN upon request in connection with contractual obligations.

We commit to maintaining reports detailing security threats or inaccurate WHOIS records, and to maintaining these reports for inspection during the agreed contracted period, once further details on said requirements are made available.

5. Making and Handling Complaints – Registry operators will ensure that there is a mechanism for making complaints to the registry operator that the WHOIS information is inaccurate or that the 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 otherwise engaging in activity contrary to applicable law.

As detailed in section 28 of our application, we commit to implementing an abuse and complaint tracking and monitoring system that will be maintained 24 hours a day, seven days a week. All registry staff will be trained in both operating the system and managing/entering complaints. This system will provide a reliable and simple way for the public to inform us if they think there is a problem. Submissions of suspected infringement or abuse are monitored by Registrar Customer Service personnel and escalated according to severity. Upon escalation, we may take immediate action to protect registry system or the public interest or refer the matter to law enforcement if we suspect criminal activity.

6. Consequences – Consistent with applicable law and any related procedures, registry operators shall ensure that there are real and immediate consequences for the demonstrated provision of false WHOIS information and violations of the requirement that the domain name should not be used in breach of applicable law; these consequences should include suspension of the domain name.

Our abuse prevention and mitigation program employs a model that includes registry-level suspensions for AUP and other policy violations, and also provides that the use of a domain is subject at all times to the AUP's provisions concerning cybercrime, prohibited content, intellectual property abuses and other issues of importance to the Internet, security, intellectual property, legal and law enforcement communities.

We reserve the right to cancel or suspend any name that in our sole judgment is in violation of the terms of service. With cancelation, to the extent permitted by applicable law, we may publish notice of the cancelation, along with a rationale for the decision.

We believe that this step is important for several reasons: (i) It will help us keep the trust of Internet users, who will see that our actions are not arbitrary; (ii) it will act as a deterrent, as violators' names will be published; and (iii) it will provide valuable additional information to users about which names are considered violations, by providing examples of names that have been canceled because they are offending terms.

In the case of clear-cut violations of the policies, we will take immediate action without refund of the registration fee.

GAC ADVICE: Consumer protection, sensitive strings, and regulated markets

Regarding the safeguards the GAC believes should apply to registries which fall under Category 1 within Annex 1 of its Beijing Communique, we believe the term 'media' and its notion of mass communication make .MEDIA a broad, generic term, and a gTLD which should enjoy the same freedom of similar, highly generic terms. That said, we appreciate the GAC's concern regarding the sensitivity of intellectual property within the new gTLD process, and therefore present the following responses to each of the GAC's five points within Annex 1 of the Beijing Communique.

1. Registry operators will include in its acceptable use policy that registrants comply with all acceptable laws, including those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, debt collection, organic farming, disclosure of data, and financial discourses.

Our AUP contains provisions enforceable to the extent that is possible under the terms of the registry agreement. As each GAC member country has individual acceptable and differing laws regarding privacy, data collection, consumer protection, fair lending, debt collection, organic farming, disclosure of data, and financial discourses, it is difficult to adhere to each country's specific laws. However, should GAC member countries achieve a suitable global standard for these, we would commit to adopting them.

We require registrars to adopt and enforce our AUP during the sales process, which includes a number of commitments and enforceable processes designed to ensure that registered domain names will be used only for legitimate activities. A non-exhaustive list is provided above in our response to safeguard #2. Our AUP also explicitly prohibits the distribution of material that violates the legal rights of others, including but not limited to rights of privacy or intellectual property protections.

2. Registry operators will require registrars at the time of registration to notify registrants of this requirement.

We will require registrars to include the notification in their condition of registration to the registrant. Moreover, registrars will be periodically audited to ensure they are able to demonstrate compliance with this requirement.

As a company with extensive experience operating a reseller channel, we are well-versed in auditing companies to ensure contractual compliance, and always take the initiative to ensure both ourselves and our partners are following best practices regarding AUPs and contracts.

3. Registry operators will require that registrants who collect and maintain sensitive health and financial data implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law and recognized industry standards.

We believe the protection of personal data and privacy is paramount, and expectations regarding the importance of this are set forth within our policies and processes. We therefore commit to establishing expectations regarding a registrant's treatment of sensitive data within our own registration agreement, to the extent that is possible as a Canadian company subject to Canada’s privacy regulations.

4. Establish a working relationship with the relevant regulatory, or industry self-regulatory, bodies, including developing a strategy to mitigate as much as possible the risks of fraudulent, and other illegal, activities.

As there are no global regulatory or self-regulatory bodies for the media industry, and given the wide-reaching, global nature of the .MEDIA extension, we do not believe there is a single, authoritative regulatory body in which to establish a working relationship. That said, should such an organization emerge in the future, or should ICANN mandate working with a particular organization, we would commit to doing so.

5. Registrants must be required by the registry operators to notify to them a single point of contact which must be kept up-to-date, for the 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.

At a high level, we support the notion of contacting registrants directly in the event of complaints reports or reports of registration abuse.

It should be noted that inserting the registry in the registrant-registrar relationship is a paradigm registrants, registrars and resellers are largely unfamiliar with in the gTLD space.

Should this requirement be implemented, it would be ideal to enforce it through the use of an existing contact, which is already required to be valid and up-to-date at all times, and enforced through the AUP, as opposed to introducing a new contact specifically for reaching out to registrants.

Should a single, authoritative regulatory or industry self-regulatory body be established, we also commit to publishing contact details of those relevant organizations. However, given the regional nature of regulatory and self-regulatory agencies and the global nature of .MEDIA, we do not feel there is an appropriate body at this time.