**TERMS OF USE POLICY**
Version 1.0 – 10/29/2015

## Summary

This Terms of Use Policy (the "Use Policy"), to be read together with the Registration Agreement and .HOTELES Registry Policies, sets forth the terms and conditions that Registrants must adhere to when registering and using a domain name in the TLD, as well as outlines the actions that the Registry may take to address non-compliance under this Use Policy.

## Use Policy Overview

All domain name Registrants must act responsibly in their use of any TLD domain name or website hosted on any TLD domain name, and in accordance with this policy, ICANN rules and regulations, and applicable laws, including those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, and intellectual property rights.

The Registry will not tolerate abusive, malicious, or illegal conduct in registration of a domain name; nor will the Registry tolerate such content on a website hosted on a TLD domain name.

This Use Policy will govern the Registry's actions in response to abusive, malicious, or illegal conduct of which the Registry becomes aware. In all cases the Registry reserves the right to bring the offending sites into compliance using any of the methods described herein, or others as may be necessary in the Registry's discretion, whether or not described in this Use Policy.

Upon becoming aware of impermissible conduct, the Registry (or its designees) may alert any relevant Registrar about any identified threats, and may work with them to resolve such issues. The Registry will also utilize such other methods in compliance with applicable laws and ICANN policies, as it deems appropriate.

## Use Policy Purposes

The Registry reserves the right to take appropriate actions, whether administrative, operational or otherwise, as it deems necessary, in its unlimited and sole discretion and without notice, to:

- Support the stated mission and purpose of the TLD;
- Protect the integrity, security and stability of the TLD and the Domain Name System (DNS) as a whole;

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

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

- Comply with the terms of the Registry-Registrant Agreement, the Registry Agreement, or any other binding commitments, whether written or otherwise;

- Respond to or protect against any form of malware (defined to include, without limitation, malicious code or software that might affect the operation of the TLD, the Internet or which cause direct or material harm to others);

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

- Correct mistakes made by the Registry, Registry Service Provider, or Registrar in connection with a domain name registration;

- Allow for the resolution of a dispute of any sort, whether or not the dispute appears to be unmerited or unsubstantiated;

- Respond to complaints of abusive behavior on websites hosted on the TLD;

- Address the non-payment of fees; or

- Otherwise implement the Use Policy.

**Prohibited Activities**

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

- **Botnet Command and Control**: Services run on a domain name that are used to control a collection of compromised computers or “zombies,” or to direct Distributed Denial of Service (DDoS) attacks;

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

- **Fast Flux Attacks/Hosting**: A technique used to shelter Phishing, Pharming, and Malware sites and networks from detection and to frustrate methods employed to defend against such practices, whereby the IP address associated with fraudulent sites are changed rapidly so as to make the true location of the sites difficult to find;

- **Hacking**: Unauthorized access to a computer network;

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

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

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

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

- **Activities contrary to applicable law**: Trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or other;

- **Regulatory noncompliance**: Public regulatory action taken against the Registrant for failure to comply with reasonable and appropriate security measures; and

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

- **Defamation or Inappropriate Activity**: The posting of content that goes against the stated mission and purpose of the TLD.

- Any other abusive behaviors that appear to threaten the stability, integrity or security of the Registry or any of its Registrar partners and/or that may put the security of any Registrant or user at risk, including but not limited to: cybersquatting, sale and advertising of illegal or counterfeit goods, front-running, gripe sites, deceptive and/or offensive domain names, fake renewal notices, cross gTLD registration scams, traffic diversion, false affiliation, domain kiting/tasting, fast-flux, 419 scams

**Registry's Response Plan**

The Registry will maintain a public email gtldscontact@despegar.com on its respective websites for interested third parties to submit alleged incident of abuse and/or non-compliance. Notwithstanding the foregoing, the Registry may also identify Use Policy violations by any means, including without limitation, a private complaint, public alert, government or enforcement agency outreach, ICANN notification, and on-going monitoring by the Registry or its partners. The Registry's plan to respond to allegations of abuse is based upon the following four pillars: Verification, Investigation, Remediation and Follow-up as identified in more detail below:

- **Verification**: The Registry will use commercially reasonable efforts, including contracting with a third-party technical partner, to review all submissions and make an initial determination regarding the source and legitimacy of each submission. At its discretion, the Registry or its designee, through an automated system or otherwise, may view any website hosted on a TLD domain name, for the purpose of identifying and verifying Use Policy violations.

- **Investigation**: The Registry will prioritize all investigations in the following order:
    1. Law enforcement complaints (within twenty-four (24) hours);
    2. Third party security, stability or criminal complaints (within one (1) business day); and
    3. Third party non-security, non-stability, or non-criminal complaints (within five (5) business days).

  Registry will endeavor to investigate the highest priority incidents within twenty-four (24) hours and the lower priority incidents in five (5) business days.

- **Remediation**: As a result of any investigation involving credible complaints or violations of law in matters pertaining to security, stability or criminal activity, the Registry will endeavor to take appropriate action within twelve (12) hours of completing an initial investigation. In all other complaints not involving security, stability or criminal activity, the Registry will seek to resolve the matter through an escalated notification process: email, telephone, certified mail.

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

**Actions The Registry May Take**
To enforce this Use Policy, including Responding to any prohibited activities or to effectuate the policy purposes described above, the Registry may take actions including but not limited to:

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

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

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

- 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;

- Cancel or transfer or take ownership of any domain name, either temporarily or permanently;

- Deny attempted registrations from repeat violators;

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

- 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.

The Registry may also take preventative measures at its sole discretion including (without limitation):

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

- Removal of orphan glue records; and

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

**Amendment**
The Registry reserves the right to modify this Use Policy at its sole discretion in accordance with its rights and obligations set forth in its Registry Agreement. Such revised Use Policy shall be posted on Registry's website at www.nic.HOTELES at least 30-calendar days before its effective date.