.ONL Anti-Abuse Policy

The following policy (“I-REGISTRY Ltd. Anti-Abuse Policy") is announced pursuant to the Registry-Registrar-Agreement (“RRA”) and is effective upon thirty days' notice by I-REGISTRY Ltd. (“Registry”) to Registrars. Abusive use(s) of .ONL domain names should not be tolerated.

The policy includes the general aspects of anti-abuse, acceptable use and rapid takedown and applies to registrars and registrants of .ONL domain names and defines how the Registry will proceed if abuses that are reported to the Registry. The policy does not replace the Uniform Dispute Resolution Policy (UDRP) or Uniform Rapid Suspension (URS) or other proceedings for disputes.

The Registry, together with the Registry-Service-Provider, will take the requisite operational and technical steps to promote WHOIS data accuracy, limit domain abuse, remove outdated and inaccurate data, and other security measures to ensure the integrity of the TLD. The specific measures include, but are not limited to a TLD Anti-Abuse Policy that clearly defines abuse, and provide point-of-contact information for reporting suspected abuse, committing to rapid identification and resolution of abuse, including suspensions, ensuring completeness of WHOIS information at the time of registration, publishing and maintaining procedures for removing orphan glue records for names removed from the zone, and establishing measures to deter WHOIS abuse, including rate-limiting, determining data syntax validity, and implementing and enforcing requirements from the Registry-Registrar Agreement.

Acceptable Use of .ONL Domain Names

The Registry intends that no domain name in the .ONL space shall be used in a manner which, infringes any other third parties’ rights, is in breach with any applicable laws, government rules or requirements or for the purposes of undertaking any illegal or fraudulent actions, including spam or phishing activities.

Failure to comply with the above provisions may result in the suspension or termination of the domain name registration by the Registry.

Abuses of .ONL Domain Names

The nature of such abuses creates security and stability issues for the Registry, registrars and registrants, as well as for users of the Internet in general. The Registry’s definition of abusive use of a .ONL domain name includes, without limitation, the following:

- Illegal or fraudulent actions;
- 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 the spamming of Web sites and Internet forums;

- Phishing: The use of 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 unknowing users to fraudulent sites or services, typically through, but not limited to, DNS hijacking or poisoning;
- Willful distribution of malware: The dissemination of software designed to infiltrate or damage a computer system without the owner's informed consent. Examples include, without limitation, computer viruses, worms, keyloggers, and Trojan horses.
- Malicious fast-flux hosting: Use of fast-flux techniques with a botnet to disguise the location of web sites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities.
- 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 attacks (DDoS attacks);
- Distribution of child pornography; and
- Illegal Access to Other Computers or Networks: Illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system (often known as "hacking"). Also, any activity that might be used as a precursor to an attempted system penetration (e.g., port scan, stealth scan, or other information gathering activity).

Rapid Takedown of .ONL Domain Names

The Registry reserves the right to deny, cancel or transfer any registration or transaction that it deems necessary, in its discretion; (1) to protect the integrity and stability of the Registry; (2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, in compliance with any dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of the Registry, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) for violations of this Agreement and its Exhibits; or (5) to correct mistakes made by the Registry or any Registrar in connection with a domain name registration. The Registry also reserves the right to place a domain name on hold, lock, or similar status during resolution of a dispute.

If a registrar does not take action within a time period indicated by the Registry (usually 24 hours), the Registry might then decide to take action itself. At all times, the Registry reserves the right to act directly and immediately if the potential harm to Internet users seems significant or imminent, with or without notice to the sponsoring registrar.

The Registry will be prepared to call upon relevant law enforcement bodies as needed. There are certain cases, for example, Illegal pharmacy domains, where the Registry will contact the Law Enforcement Agencies to share information about these domains, provide all the evidence collected and work closely with them before any action will be taken for suspension. The specific action is often dependent upon the jurisdiction of which the Registry, although the operator in all cases will adhere to applicable laws and regulations.

When valid court orders or seizure warrants are received from courts or law enforcement agencies of relevant jurisdiction, the Registry will order execution in an expedited fashion. Compliance with these will be a top priority and will be completed as soon as possible and within the defined time-lines of the order. There are certain cases where Law Enforcement Agencies request information about a domain including but not limited to:

- Registration information
- History of a domain, including recent updates made
- Other domains associated with a registrant's account
- Patterns of registrant portfolio

Requests for such information is handled on a priority basis and sent back to the requestor as soon as possible. The Registry sets a goal to respond to such requests within 24 hours.

The Registry may also engage in proactive screening of its zone for malicious use of the domains in the gTLD, and report problems to the sponsoring registrars. The Registry could take advantage of a combination of the following resources, among others:

- Blocklists of domain names and name servers published by organizations such as SURBL and Spamhaus.
- Anti-phishing feeds, which will provide URLs of compromised and maliciously registered domains being used for phishing.
- Analysis of registration or DNS query data [DNS query data received by the gTLD name servers.]

The Registry will keep records and track metrics regarding abuse and abuse reports. These will include:

- Number of abuse reports received by the Registry's abuse point of contact described above;
- Number of cases and domains referred to registrars for resolution;
- Number of cases and domains where the Registry took direct action;
- Resolution times;
- Number of domains in the gTLD that have been blacklisted by major anti-spam blocklist providers, and;
- Phishing site uptimes in the gTLD.

Removal of orphan glue records

By definition, orphan glue records used to be glue records. Glue records are related to delegations and are necessary to guide iterative resolvers to delegated name servers. A glue record becomes an orphan when its parent name server record is removed without also removing the corresponding glue record. (Please reference the ICANN SSAC paper SAC048 at: http://www.icann.org/en/committees/security/sac048.pdf.) Orphan glue records may be created when a domain (example1.tld) is placed on EPP ServerHold or ClientHold status. When placed on Hold, the domain is removed from the zone and will stop resolving. However, any child name servers

(now orphan glue) of that domain (e.g., ns1.example1.tld) are left in the zone. It is important to keep these orphan glue records in the zone so that any innocent sites using that name server will continue to resolve. This use of Hold status is an essential tool for suspending malicious domains.

The Registry, together with the Registry-Service-Provider, observes the following procedures, which are being followed by other registries and are generally accepted as DNS best practices. These procedures are also in keeping with ICANN SSAC recommendations.

When a request to delete a domain is received from a registrar, the Registry first checks for the existence of glue records. If glue records exist, the Registry will check to see if other domains in the Registry are using the glue records. If other domains in the Registry are using the glue records then the request to delete the domain will fail until no other domains are using the glue records. If no other domains in the Registry are using the glue records then the glue records will be removed before the request to delete the domain is satisfied. If no glue records exist then the request to delete the domain will be satisfied.

If a registrar cannot delete a domain because of the existence of glue records that are being used by other domains, then the registrar may refer to the zone file or the "weekly domain hosted by name server report" to find out which domains are using the name server in question and attempt to contact the corresponding registrar to request that they stop using the name server in the glue record. The Registry does not plan on performing mass updates of the associated DNS records.

The Registry will accept, evaluate, and respond appropriately to complaints that orphan glue is being used maliciously. Such reports should be made in writing to the Registry, and may be submitted to the Registry's abuse point-of-contact. If it is confirmed that an orphan glue record is being used in connection with malicious conduct, the Registry will have the orphan glue record removed from the zone file. The Registry has the technical ability to execute such requests as needed via its Registry-Service-Provider.

Methods to promote WHOIS accuracy

The creation and maintenance of accurate WHOIS records is an important part of Registry management. The Registry will manage a secure, robust and searchable WHOIS service for this gTLD.

Contacts

All reports of abuse should be sent to abuse@nic.onl.

Any complaints regarding inaccurate WHOIS information or should be addressed to the sponsoring registrar of that domain. Complaints may also be sent to support@nic.onl.