Acceptable Use Policy

Summary

This policy describes the Acceptable Use of domain names for .Med licensees. Licensees must adhere to this policy in order to retain the use of the license. This policy outlines the reservation of rights that Medistry LLC retains in order to address non-compliance.

Acceptable Use of .Med Domains

Medistry LLC's Reservation of Rights

Medistry LLC reserves the right to deny, cancel or transfer any registration or transaction, or place any domain name on registry lock, hold or similar status, as it deems necessary, in its unlimited and sole discretion and without notice, either temporarily or permanently:

- To protect the integrity, security and stability of the Domain Name system (DNS);
- To 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;
- To avoid any liability, civil or criminal, on the part of Medistry LLC, as well as its affiliates, subsidiaries, officers, directors, employees and members;
- To enforce all Requirements and Policies as posted on the Medistry LLC's website
- To 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 Internet or which cause direct or material harm to others);
- To comply with specifications adopted by any industry group generally recognized as authoritative with respect to the Internet (e.g., Requests for Comments (RFCs));
- To correct mistakes made by Medistry LLC, Registry Service Provider, or Registrar in connection with a domain name registration; or
- For the non-payment of fees.

Licensee Obligations

Licensees of all .Med domains are required:

- To comply with all applicable Requirements and Policies posted on Medistry LLC's website at www.trust.med/policies

- To comply with their End User License Agreement (EULA);

- To notify Medistry LLC via email to abuse@trust.med or via the telephone contact listed at our website (www.trust.med) within one (1) business day if public regulatory action has been taken against them for failure to comply with reasonable and appropriate security measures or that has resulted in the revocation the credential or license which was used to certify their eligibility to License a .Med domain; and

- To comply with the following obligations, imposed by ICANN, in connection with its Governmental Advisory Committee Advice:

    - Maintain accurate and up-to-date WHOIS information to receive 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;

    - Report any material changes to the validity of Registrant's authorizations, credentials, licenses and/or other related credentials for participation in in order to ensure they continue to conform to appropriate regulations and licensing requirements and generally conduct their activities in the interests of the consumers they serve;

    - Comply with all applicable laws, including those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct);

    - Implement reasonable and appropriate security measures commensurate with the offering of healthcare services, as defined by applicable law within their jurisdiction.

- To operate their .Med domain in a safe and secure manner utilizing the strongest possible technical security measures available to ensure compliance with jurisdictional laws, safe computing standards, or other standards considered best practice within your segment of the healthcare ecosystem ("Security Requirements"). In particular, all .Med domains must operate with:

    - DNSSEC enabled at each zone and subsequent sub-zones for domains that resolve in the DNS to ensure a chain of trust is established for all .Med domain names. Licensee shall follow the best practices described in RFC 6781[1].

    - DNS Resource Records (e.g., CNAME, DNAME, SRV) are prohibited from aliasing to DNS records outside of the secure zone to ensure traditional DNS zones may not impersonate higher security DNS zones (including all sub-domains).

[1] https://tools.ietf.org/html/rfc6781

- A valid Domain-based Message Authentication, Reporting and Conformance (DMARC) record must be published with a requested mail receiver policy of either "quarantine" or "reject" for domains that resolve in the DNS. For .Med domains intended to send email, Licensees must publish at least one of the following email authentication DNS Resource Records:
    - Sender Policy Framework (SPF), or
    - Domain Keys Identified Mail (DKIM)

  When used to protect non-email sending domains, Registrants are required to publish a DMARC reject requested mail receiver policy.

- Name server host names are within the parent zone to ensure authoritative name servers are trusted and verifiable.

- Transport Layer Security (TLS) implemented using trusted protocol versions to protect the integrity and confidentiality of data in-transit. TLS 1.1 or greater must be used due to vulnerability in other versions. Reference RFC 5746[2] for guidelines on implementation. The following non-exhaustive list of cipher suite components (authentication, encryption, message authentication code and key exchange algorithms) are excluded from use within the secure zone and the generation of TLS certificates:
    - Anon, DES, 3DES, FIPS, GOST 28147-89, IDEA, SEED, WITH_SEED, MD5, NULL, SHA (SHA1), RC4, EXPORT, EXPORT1024 and SRP.

- To maintain the integrity of the verification process, Medistry LLC may impose additional use restrictions and/or Security Requirements, at any time, on a Licensee's use of a domain name to protect the integrity of the community that it serves. Medistry LLC will communicate these additional use restrictions on a domain name to a Licensee before approving the initial registration request or at any time during the term of the registration and before any subsequent renewals of the domain name.

Licensee Prohibitions

The following is a non-exhaustive list of prohibitions that Licensee's accept as guidelines of conduct within the .Med namespace:

General Prohibitions

- Abusive use of any .MED domain name(s)

- Uploading, posting, or otherwise making available any content that is unlawful, harmful, abusive, threatening, invasive of another's privacy

- Damaging or amounting to harassment or cyber bullying of another person

[2] https://tools.ietf.org/html/rfc5746

- Intentional or unintentional violation of any applicable local, state, national, international or other law

- Any illegal, disruptive, malicious, or fraudulent action

Security & Trustworthy Operations Prohibitions

- 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.

- Non-healthcare oriented operations: The display, publication and/or dissemination of content or services within the .Med namespace that is not oriented towards to the intended scope of the .Med License per the application submitted.

Amendments

Medistry LLC reserves the right to modify this Policy at its sole discretion in accordance with its rights and obligations set forth in its Registry Agreement. Such revised Policy shall be posted on its website, www.trust.med/policies, at least 15-calendar days before its effective date.