The City of Stockholm Acceptable Use Policy

This Acceptable Use Policy forms an integrated part of the *General Terms & Conditions for the registration and maintenance of .stockholm Domain Names*.

The Registry is committed to maintaining the .stockholm space as a safe and secure online environment; and prevent all malicious, illegal or fraudulent use of Domain Names; and limit the potential for significant harm to Internet users. The purpose of this policy is to allow the Registry and its Accredited Registrars to investigate and to take swift action in case of abusive use and to deter registrants from engaging in illegal or fraudulent use of Domain Names in the .stockholm TLD.

1 Lawful use

A registrant may only use a Domain Name for lawful purposes.

2 Compliance with City Council policies and other regulations

The content of websites under the .stockholm domain must comply with the goals stated by City Council. Regulations outlined by The City of Stockholm's IT Security Policy must be followed as well as technical security measures determined in The City of Stockholm's IT-program. Integrity issues regarding handling and presentation of personal data must follow national regulations (Personal Data Act, PUL) The City of Stockholm name-servers must be used for all Domain Names under the new gTLD.

3 Abusive use

A Domain Name must not be used to publish content or otherwise that constitutes abusive use. 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 City of Stockholm defines abusive use as the wrong or excessive use of power, position or ability, and 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 e-mail spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of Websites and Internet forums. An example, for purposes of illustration, would be the use of email in denial-of-service attacks;
- **Phishing:** The use of counterfeit Web pages that are designed to trick recipients into divulging sensitive data such as usernames, passwords, or financial data;
- **Pharming:** The redirecting of unknowing users to fraudulent sites or services, typically through 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;
- **Fast flux hosting:** Use of fast-flux techniques to disguise the location of Websites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities. Fast-flux techniques use DNS to frequently change the location on the Internet to which the Domain Name of an Internet host or name server resolves. Fast flux hosting may be used only with prior permission of The City of Stockholm;
- **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 denial-of-service attacks (DoS attacks);
- **Distribution of child pornography;**
- **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); and
- **Willful disregard of quality control measures**: Repetitive disregard of reporting measures such as analytics follow-ups and on-page quality standards.

4 Prohibited content

A Domain Name must not be used to publish, distribute or communicate (including through links forwarding or framing):

- material that infringes on intellectual property rights of other persons – including trademarks, copyrights, patents, trade secrets etc.;
- images or materials that are prohibited by or constitute an offense under applicable laws;
- material that includes real or manipulated images depicting the sexual exploitation of children;
- material containing threats or detailed instructions regarding how to commit a crime or encourages conduct that may constitute a criminal offence;
- defamatory material or material that constitutes racial vilification or “hate speech”; or
- material that otherwise is contrary to the public safety or order.

5 Reporting abuse

Any abuse involving Domain Names can be reported at abuse@nic.stockholm, including reports of illegal activity.

The Registry will then work in cooperation with the relevant Registrar to rapidly address identified threats or confirmed abuse complaints, investigate all reasonable complaints, and take any appropriate action(s) thereto.

The Registry will implement all valid court orders or seizure warrants from courts, arbitration tribunals, or law enforcement agencies of applicable jurisdictions, provided the court orders and seizure warrants are enforceable at the domicile of the Registry. The Registry will work closely together with law enforcement agencies if necessary and provide them with an additional, fast track access to the abuse point of contact.

6 Enforcement

As set out in the General Terms and Conditions the Registry may (but is not obliged to), in its sole discretion (including based on reports made to the Registry by third parties), and without prior notification, suspend, transfer, or terminate a registrant's service, including all and any of the registrant's Domain Name registrations, if the Registry believes:

1) that a violation of this Acceptable Use Policy or any other Registry Policy has occurred or a reasonable indication that such a violation may have occurred; and/or
2) that a suspension and/or termination may otherwise be in the public interest.