.SS Domain Anti-Abuse policy

Malicious use of .SS domain names is prohibited as per the Registration Policy and the Terms & Conditions of registering a .ss domain name. 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. ssNIC defines abusive use of a domain 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 personal 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, computer contaminant, worms, keyloggers, and Trojans.
- **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).
- **Publishing or transmitting 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).

Pursuant to the Registry-Registrar Agreement, ssNIC reserves the right at its sole discretion to deny, cancel, or transfer any registration or transaction, or place any domain name(s) on registry lock, hold, or similar status, that it deems necessary:

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, or any dispute resolution process;
3. to avoid any liability, administrative, civil or criminal, on the part of ssNIC, as well as its affiliates, agents, subsidiaries, officers, directors, and employees;
4. per the terms of the registration agreement and this Anti-Abuse Policy, or
5. to correct any mistakes made by ssNIC or any registrar in connection with a domain name registration. ssNIC also reserves the right to place upon registry lock, hold, or similar status a domain name during resolution of a dispute.

All reports of abuse should be sent to abuse@registry.ss