



.CAM Anti-Abuse Policy

The .CAM TLD registry (".CAM") is committed to the stable and secure operation of the .CAM top-level domain ("TLD"). Abusive use of domain names creates security and stability issues for registries, registrars and registrants - as well as for users of the Internet in general. Accordingly, .CAM requires that domain names in its TLDs adhere to this Anti-Abuse Policy ("AAP").

1. .CAM will address abusive behavior in its TLDs consistent with this policy. .CAM provides an abuse point of contact through an e-mail address posted on the .CAM website found at <https://NIC.cam>. This e-mail address will allow our staff to monitor and address abuse reports. .CAM also provides a web form for complaints on our website <https://NIC.cam>.
2. .CAM reserves the right, at its sole discretion and at any time and without limitation, to deny, suspend, cancel, redirect, or transfer any registration or transaction, or place any domain name(s) on registry lock, hold, or similar status as it determines necessary for any abusive use of a .CAM domain name, including without limitation any of the following:
 - to protect the integrity and stability of one of the .CAM registry;
 - to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process;
 - to avoid any liability, civil or criminal, on the part of .CAM, its affiliates, subsidiaries, officers, directors, contracted parties, agents, or employees;
 - to comply with the terms of the applicable registration agreement and .CAM policies;
 - where registrant fails to keep Whois information accurate or up-to-date;
 - domain name use is abusive or violates this policy, or a third party's rights or acceptable use policies, including but not limited to the infringement of any copyright or trademark;
 - to correct mistakes made by a registry operator or any registrar in connection with a domain name registration; or,
 - as needed during resolution of a dispute.



3. Abusive use of a domain (including domain name itself) is described as any illegal, disruptive, malicious, or fraudulent action and includes, without limitation, the following:
 - distribution of malware;
 - dissemination of software designed to infiltrate or damage a computer system without the owners informed consent, including, without limitation, computer viruses, worms, keyloggers, trojans, and fake antivirus products;
 - phishing, or any attempt to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication;
 - DNS hijacking or poisoning;
 - spam, including using electronic messaging systems to send unsolicited bulk messages, including but not limited to e-mail spam, instant messaging spam, mobile messaging spam, and the spamming of Internet forums;
 - botnets, including malicious fast-flux hosting;
 - denial-of-service attacks;
 - child pornography or any images of child abuse, including (but not limited to) terms that may depict underage persons like “girl”;
 - promotion of escort services or any term we deem as a front for prostitution;
 - activities related to or depicting terrorism, terrorist organizations or terrorists names;
 - promotion, encouragement, sale, or distribution of prescription medication without a valid prescription in violation of applicable law; • illegal access of computers or networks; and,
 - cyber-bullying or harassment.

4. .CAM is committed to ensure that registrants of a letter/letter two-character ASCII label will not misrepresent or falsely imply that the registrant or its business is affiliated with a government or country-code manager if such affiliation, sponsorship or endorsement does not exist.

Updated **Thursday, Nov 14th, 2024**