

Generic Anti-Abuse Policy

Published by: [DNS Abuse Institute](#)

This Anti-Abuse Policy is established for all domain name registrations for which [NAME] serves as the [Registrar/Registry Operator]. This Policy focuses on technical abuses of the Domain Name System (DNS) (“DNS Abuse”). [The Registrar/Registry is also free to detail categories of Website Content questions it addresses, such as Child Sexual Abuse Materials]

DNS Abuse

DNS Abuse causes security and stability issues for domain name Registrars, Registry Operators, Registrants and users of the Internet as a whole. This Anti-Abuse Policy prohibits the following technical abuses¹ in [Registrar/Registry Operator’s] domain name registrations:

- **Malware** is malicious software, installed on a device without the user’s consent, which disrupts the device’s operations, gathers sensitive information, and/or gains access to private computer systems. Malware includes viruses, spyware, ransomware, and other unwanted software.
- **Botnets** are collections of Internet-connected computers that have been infected with malware and commanded to perform activities under the control of a remote administrator.
- **Phishing** occurs when an attacker tricks a victim into revealing sensitive personal, corporate, or financial information (e.g. account numbers, login IDs, passwords), whether through fraudulent or ‘look-alike’ emails, or luring end users to copycat websites. Some phishing campaigns aim to persuade the user to install software, which is in fact malware.
- **Other technical abuses of the DNS** that may reasonably be perceived to impact the stability or security of the DNS or the [Registrar/Registry Operator’s] domain name registrations (e.g., pharming, fast flux hosting, and illegal access to other computers or networks).

¹ The definitions for Malware, Botnets, Phishing, and Spam are from the [Framework to Address Abuse](#), which relies on the definitions provided by the Internet and Jurisdiction Policy Network’s [Operational Approaches, Norms, Criteria, Mechanisms](#).

- **Spam** is unsolicited bulk email, where the recipient has not granted permission for the message to be sent, and where the message was sent as part of a larger collection of messages, all having substantively identical content. Spam is not unto itself DNS Abuse, but is included as a category under this Policy for the instances when Spam serves as a delivery mechanism for the other forms of DNS Abuse.

Actions under this Policy

[Registrar/Registry Operator] reserves the right to take appropriate action for any domain it determines violates this Policy, including the right to deny, cancel, or transfer any registration or transaction, or place any domain name on [Registrar/Registry Operator] lock, hold, or similar status, that it deems necessary in its discretion:

1. That violates the terms of this Anti-Abuse Policy;
2. To protect the integrity and stability of [Registrar/Registry Operator's] domain name registrations;
3. To comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; or
4. To avoid any liability, civil or criminal, on the part of [Registrar/Registry Operator], its affiliates, subsidiaries, officers, directors, and employees.