ACCEPTABLE USE AND ANTI-ABUSE POLICY

Last Updated On: August 25th, 2026

General Provisions

1. Namify Domain Inc. ("Namify") is committed to the stable and secure operation of its top-level domains ("TLDs"). 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, Namify requires that every domain name in its TLDs ("Registered Name") and Registered Name Holder adhere to this Acceptable Use and Anti-Abuse Policy ("AUP"). For the purpose of this AUP, a "Registered Name Holder" refers to the person or company owning or otherwise controlling a Registered Name by virtue of a registration agreement with a registrar.

2. Every Registered Name Holder is required to enter into and comply with a registration agreement with an ICANN-Accredited registrar or its authorized representative.

3. Every Registered Name Holder is required to comply with all ICANN consensus policies applicable to Registered Name Holders, including (a) the Uniform Domain Name Dispute Resolution Policy (http://www.icann.org/en/help/dndr/udrp and (b) the Uniform Rapid Suspension Policy (http://newgtlds.icann.org/en/applicants/urs), and (c) such other ICANN consensus policies as ICANN publishes on its website and makes applicable to Namify, Registrars or Registered Name Holders, and as may be amended by ICANN from time to time.

4. Every Registered Name Holder acknowledges and agrees that Registered Name Holders are solely responsible for the content they publish on websites on the Registered Name. Namify cannot and does not design, review or screen content on any website and does not assume any obligation to monitor such content. However, each Registered Name Holder agrees that Namify may review websites or other content in responding to a third-party complaint or for any other reason.

5. By applying for or obtaining a Registered Name, every Registered Name Holder acknowledges, accepts, and agrees to comply with the terms under which such application and registration were made, including the terms and conditions of all other applicable policies available on the Namify website and use restrictions set forth herein.

6. Registered Name Holders who have obtained or registered any two-character second-level domain name/s under any of the TLDs will take steps to ensure against misrepresenting or falsely implying that the Registered Name Holder or its business is affiliated with a government or country-code manager if such affiliation, sponsorship or endorsement does not exist.

7. Namify reserves the right to deny, suspend, cancel, delete, redirect, or transfer any registration or transaction or place any Registered Name(s) on registry lock, hold, or similar status that it deems necessary, in its sole discretion, for any of the following reasons:

* to protect the integrity and stability of the 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 Namify, as well as its affiliates, subsidiaries, officers, directors, contracted parties, agents, or employees;
* to comply with the terms of the applicable registration agreement and Namify policies;
* where the Registered Name Holder fails to keep Whois information accurate or up-to-date;
* Registered Name use is abusive or violates the AUP or a third party's rights or acceptable use policies, including but not limited to the infringement of any copyright or trademark;
* where the Registered Name is found to have been registered as part of a set of any pattern-based registration that has shown abusive trends in the past or is part of a present or ongoing abusive campaign, including but not limited to domains registered using any domain generation algorithms, scripts, dictionaries, etc., detected by Namify;

* to correct mistakes made by Namify in connection with the registration of a Registered Name; or
* as needed during the resolution of a dispute.

8. Namify reserves the right to disclose individual non-public personal data of Registered Name Holders associated with Registered Names which are found to be in violation of this AUP and/or if required or requested by law enforcement agencies, security agencies, registries, and other service providers irrespective of the number and frequency of AUP violations.

Prohibited Uses

The following will be deemed as violations of the AUP:

1. Intellectual property, Trademark, Copyright, and Patent violations, including piracy
Common types of intellectual property rights include copyrights, trademarks, patents, industrial design rights, and trade secrets in recognized jurisdictions. Any act resulting in theft, misuse, misrepresentation, or any other harmful act by any Registered Name Holder will be categorized as an Intellectual Property violation.

2. Cybersquatting
Cybersquatting refers to the registration or acquisition of domain names that are identical or confusingly similar to a registered trademark or service mark held by a third party in circumstances indicating that the Registered Name Holder registered the domain name (i) primarily for the purpose of selling, renting, or transferring the domain name to the owner of the trademark or service mark for consideration higher than the registration cost incurred by the Registered Name Holder or (ii) in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name (including by combining second and third-level subdomains) or (iii) primarily for the purpose of disrupting the business of the trademark or service mark holder or (iv) in an attempt to attract, for commercial gain, Internet users to the registered domain name/website or other online location by creating a likelihood of confusion with the trademark or service mark as to the source, sponsorship, affiliation, or endorsement of the website or a product or service on the website.

3. Spamming
Spamming refers to 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 Web sites and Internet forums. Unsolicited emails advertising legitimate and illegitimate products, services, and/or charitable requests and requests for assistance are also considered spam.

4. Phishing (and various forms of identity theft)
Fraudulent web services and applications meant to represent/confuse or mislead internet users into believing they represent services or products for nefarious purposes, such as illegally gaining login credentials to actual legitimate services.

5. Pharming and DNS hijacking
This includes redirection of DNS traffic from legitimate and intended destinations, by compromising the integrity of the relevant DNS systems. This leads unsuspecting Internet users to fraudulent web services and applications for nefarious purposes, such as illegally gaining login credentials to actual legitimate services.

6. Distribution of viruses or malware
Most typically the result of a security-compromised web service where the perpetrator has installed a virus or "malevolent" piece of software meant to infect computers attempting to use the web service in turn. Infected computers are then security compromised for various nefarious purposes, such as gaining stored security credentials or personal identity information such as credit card data. Additionally, compromised computers can sometimes be remotely controlled to inflict harm on other internet services.

7 . Child pornography
Refers to images or films (also known as child abuse images) and, in some cases, writings depicting sexually explicit activities involving a minor.

8. Using Fast Flux techniques

A methodology for hiding multiple source computers delivering malware, phishing, or other harmful services behind a single domain hostname by rapidly rotating associated IP addresses of the sources computers through related rapid DNS changes. This is typically done at DNS zones delegated below the level of a TLD DNS zone.

9. Running Botnet command and control operations
A Botnet is a significant coordinated net of compromised (sometimes tens of thousands) computers running software services to enact various forms of harm - ranging from unsanctioned spam to placing undue transaction traffic on valid computer services such as DNS or web services. Command and control refers to a smaller number of computers that issue/distribute subsequent commands to the Botnet. Compromised Botnet computers will periodically check in with a command and control computer that hides behind a list of date-triggered, rotating domain registrations, which are pre-loaded in the compromised computer during its last check-in.

10. Hacking
Hacking constitutes illegally accessing computers, accounts, or networks belonging to another party or attempting to penetrate the security measures of other individuals. It also includes any activity that might be used as a precursor to an attempted system penetration.

11. Financial and other confidence scams
Financial scams, including but not limited to the cases defined below, are operated by fraudsters to lure investors into fraudulent money making schemes. Prominent examples that will be treated as abusive are

* Ponzi Schemes: A Ponzi scheme is essentially an investment fraud wherein the operator promises high financial returns or dividends that are not available through traditional investments. Instead of investing victims? funds, the operator pays "dividends" to initial investors using the principle amounts "invested" by subsequent investors. The scheme generally falls apart when the operator flees with all of the proceeds or when a sufficient number of new investors cannot be found to allow the continued payment of "dividends."
* Money Laundering: Money laundering, the metaphorical "cleaning of money" with regard to appearances in law, is the practice of engaging in specific financial transactions in order to conceal the identity, source, and/or destination of money and is a main operation of the underground economy.
* 419 Scams: "419" scam (aka "Nigeria scam" or "West African" scam) is a type of fraud named after an article of the Nigerian penal code under which it is prosecuted. It is also known as "Advance Fee Fraud". The scam format is to get the victim to send cash (or other items of value) upfront by promising them a large amount of money they would receive later if they cooperate.

12. Illegal pharmaceutical distribution
Distribution and promotion of drugs, locally within a nation or overseas, without prescription and appropriate licenses as required in the country of distribution, are termed illegal.

13. SEO Poisoning
SEO Poisoning, also known as search poisoning, is an attack method in which cybercriminals create malicious websites and use search engine optimization tactics to make them show up more prominently in search results.

14. Sale of Fake / Counterfeit Products
This includes the creation of storefronts or websites selling/offering or purporting to sell/offer any fake or counterfeit products or services.

15. Other violations
Other violations that will be expressly prohibited under the TLDs include:

* Network attacks
* Violation of applicable laws, government rules and other usage policies

Reporting violations / abuse

Namify provides an abuse point of contact through an e-mail address posted on the Namify website found at https://namify.tech/abuse

Namify also provides a web form for complaints on the Namify website.

Managing violations and abuse

Namify will address abusive behaviour in its TLDs consistent with this AUP.

* Namify shall have the discretion to undertake such actions as a cancellation, deletion, transfer, locking, or suspension of a Registered Name subject to abusive uses. Such abusive uses create security and stability issues for Namify, Registered Name Holders, and users of the Internet in general. Namify defines abusive use as the wrong or excessive use of power, position, or ability and includes, without limitation, all the uses cited under "Prohibited Uses" above
* Namify also reserves the right to deny new registrations and/or suspend or delete existing registrations of names to a Registered Name Holder who has repeatedly violated the terms of this AUP in any TLD or has been identified as a known abuser or criminal by any law enforcement agency or government whether or not the violations were committed in relation to the use of a domain name or an internet transaction. Registered Name Holders, their agents, or affiliates found through the application of this AUP to have repeatedly engaged in abusive use of Registered Names may be disqualified from maintaining any Registered Names or making future registrations. This will be triggered when it is clear that a Registered Name Holder has violated the AUP an unusual number of times.

Modifications to this AUP

Namify, in its sole discretion, may modify this AUP. Any such revised policy will be posted on the Namify website at least thirty (30) calendar days before it becomes effective. Continued use of the Registered Names after the date of the modified AUP taking effect constitutes acceptance of the modification.