

User policy for Namecase services (AUP)

Premise

Failure to comply with the following AUP will result in the immediate suspension or interruption of Services (in compliance with supply conditions thereto relating. All inquiries for information regarding this very document shall be addressed by opening a specific inquiry on the following page <http://nidoma.com/en/customer/profile?tab=helpdesk> Or by sending an email to complaint@nidoma.com.

Violations

It is prohibited to use the Namecase network and services for the promotion of illegal, abusive or irresponsible actions, among the following:

- Unauthorized access or use of data, systems or networks, including attempts to probe, scan or test the vulnerability of a system or network or to violate the security measures in place or authentication without express permission granted by the system or network's owner;

- Taking part in activities that adversely interfere with the use of the Service for any user therefore, but not limited to, attacks by means of pirated software, cracks, key generators, serials, programming attacks of all types including DOS, viruses and other harmful components or deliberate attempts to overload the transmission system;

- Collection or use of e-mail addresses, names and other personal data without the consent of the person in question (including, but not limited to, spamming, phishing, internet scams, password theft, spidering);

- Collection or use of information by third parties without consent from the owner of the information;

- Use and/or dissemination of any type of false, misleading or deceptive information even by means of, as an example but not limited to, e-mail or newsgroups;

- Use of the service for distribution of software that collects or transmits fraudulent information on users;

- Use of the service for distribution of so-called "adware" software unless: (i) one is in possession of the explicit consent of the user for the download and installation of the software on the grounds that there is a clear and visible notice regarding the nature of the software; (ii) it has to do with easily removable software with the use of standard tools for such purposes, including main operating systems (such as Microsoft "ad / remove");

- Supplying information to the public (text- or graphic-based) which could damage the Namecase image through the available services

Use of system resources

Users may not utilize the service in a way that interferes with the normal operation of Namecase services. In such circumstances, Namecase may call for restoring the terms back to initial settings if such use does not conform to standards and conflicts directly, to be determined at the discretion of said company, with the practices of other users. The user consents to not utilizing defective or non-conforming equipment as in accordance with European standards, or equipment that poses potential harm to the network's integrity and/or gets in the way of the Services and/or poses risks to the physical integrity of the persons in question. Namecase does not grant any guarantee regarding the compatibility of the apparatuses and the programs (hardware and software) used by Clients with the Services, given that all relevant verification is done at the expense of the Client.

Commercial emailing.

The dissemination of commercial messages is strictly prohibited if it does not include the following terms:

- the recipients have already given their consent in receiving such electronic e-mail by means of express opt-in consent;

- the procedures for gaining consent must include adequate tools that guarantee the persons in question are indeed the owner of the e-mail address that has provided consent;

- proof of the recipient's consent must be preserved in a method that is readily available upon request, with the obligation of the recipient of these Namecase requests to show such proof within 72 hours of receiving said request;

- procedures allowing for the revoking of a recipient's request are in place, such as, but not limited to, a link in the e-mail's body or instructions including the word "Remove" in the subject line, allowing for withdrawal of consent within 48 hours of receipt, informing the recipients that their withdrawal shall be processed within 48 hours;

- an e-mail address is always available for complaints, located in a highly visible area on all websites associated with the e-mail, and a highly effective response system detects e-mails as soon as they are sent to the given address;

It is forbidden to black out the e-mail's sender in any form. The sender's e-mail address must appear in the message's body or in the "From" line of the e-mail;

Such requirements shall be applied to messages sent by means of the Service, or for messages sent by means of any network belonging to the user or any person directly or indirectly on behalf of the recipient of a site hosted by the Services. Furthermore, it will not be possible to use a "third party" e-mail service that does not apply similar procedures to all its clients. These requirements shall be applied in the same measures as the distribution lists created by third parties as if the list had been created by the Client. Namecase reserves the right to verify and monitor whenever need be to check up on the aforementioned regulations, as well as upon request for sample information by means of opt-in method. Namecase may suspend the transmission of e-mail messages that violate the above regulations.

SMTP Authentication – Policy

Upon completion of the above regulations, it is prohibited to send emails on the SMTP Namecase servers which contain more than two hundred and fifty (250) recipients.

Attempts to get around this limitation by creating more accounts or any other means of action will be interpreted as a violation of the said restriction.

Namecase reserves the right to suspend the transmission of messages that violate such regulations. Furthermore, the email services will be discontinued or banned if a violation of the AUP policy is flagged, in compliance with the general supplier conditions.

Mail Relay

In general, mass or commercial information transmissions via email are not allowed when sent to over 5,000 (five thousand) users in a day with an average of 250 messages every 20 minutes. If sending over 5,000 messages in a day is desired, please contact our support team for further information.

Vulnerability test

The user is not allowed in any which way to probe, scan, penetrate or test the vulnerability of the Namecase network system or to violate Namecase security or the relative authentication procedures, whether with passive or invasive technique, without the express written consent from Namecase, nor can it, in the same way, perform said activities by means of services supplied by Namecase

User policy for Namecase services (AUP)

towards networks and/or Third Party systems without their explicit consent.

Newsgroups, discussion forums, other networks

The Client is aware and accepts that the content of commercial messages, messages on any sort of electronic wall, group chat or other forums that he/she participates in, for example but not limited to IRC and USENET groups, will be subject to abiding by the laws and regulations in effect. Additionally, the aforementioned person shall abide by the rules of any other network (network or circuit) which it is a user of or takes part in under the Namecase services.

Offensive content

It is strictly forbidden to publish, transmit or store on or by means of the Namecase network and apparatuses any content or links directed to content that Namecase reasonably holds:

- to build, disfigure, favorite, promote or refer to in any way pedophilia, racism, fanaticism, or to pornographic contents that are not in accordance with the rules in effect and are only accessible to those of legal age;
- to be excessively violent, incite violence, contain threats, molesting or expressions of hate;
- to be unfair or deceptive when compared to consumer protection laws in any jurisdiction, including chain letters and pyramid schemes;
- to be derogatory or violate someone's privacy;
- to put the security or health of someone at risk, to put public security and health at risk, to compromise national security or interfere with judicial investigations;
- to divulge commercial secrets or private or third party ownership information in inappropriate ways;
- to have the purpose of helping third parties elude copyright laws;
- to violate third-party copyrights, brands, patents or others' property rights;
- to promote illegal drugs, violate export control laws, make reference to illegal gambling or illegal arms trafficking;
- to be otherwise illegal or solicit an illegal behavior as per applicable law in the relative jurisdiction, of the Client or of Namecase;
- to be otherwise harmful, fraudulent or able to call for legal action against Namecase.

For content "published or transmitted" through the Namecase infrastructure or network, we include contents regarding Web, email, chat and any other type of publication or internet-based transmission.

Copyright-protected material

It is prohibited to use the Namecase network for downloading, publishing, distributing, copying or using in any way forms of text, music, software, art, imagery or other work protected by the author's rights with the exception of the below cases:

- it was expressly authorized by the holder of the rights;
- it was otherwise consented to by copyright laws in effect in the given jurisdiction.

Final provisions

- The Client shall communicate the personal data to Namecase that is necessary for the complete and correct execution of the contract; he/she guarantees, furthermore, under his/her own personal and exclusive responsibilities, that the aforementioned data is correct, updated and reflective of his/her true identity. The Client shall communicate all variances of the data to Namecase, in timely fashion and within but no later than 15 (fifteen) days from the aforementioned

variation, and also to provide in any moment, upon Namecase's request, the necessary proof of identity, of home or place of residence and, if necessary, status as a legal representative of the juridical applicant or registrant of the Service. Upon receipt of said communication, Namecase may request that the Client provide additional direct documentation in order to show the communicated variances.

In the event that the Client fails to provide Namecase with the aforementioned requested communication or documentation, or in the event that the data provided to Namecase has been detected as false, outdated or incomplete or data that Namecase has reason, at its own discretion, to believe so, Namecase reserves the right to:

- a) refuse the request forwarded by the Client concerning how to proceed regarding the Service;
- b) block services immediately, without warning and for an indefinite period;
- c) cancel and/or freeze the ability to edit data associated with the Service without warning;
- d) terminate the contract

- the client consents that if the public IP addresses assigned to their account are henceforth entered into a black-list (abusive databases) such as those published on <http://www.spamhaus.org>, there will be an automatic violation of this very AUP;

consequently, Namecase shall adopt all measures deemed necessary to protect their own IPs, including freezing and/or eliminating service, regardless of whether the IP has been reported/entered into the black-list for reasons attributed to the Client;

- the client consents that they may be placed in quarantine or have their stored data terminated on a shared system if said data have been affected by a virus or otherwise corrupted, and have, at Namecase's discretion, the ability to damage or affect the system or data from other Clients that have been entered in the same infrastructure.

- The Client shall observe the rules regarding proper use from the communal network resources labeled as "Netiquette",