

NASSTAR



# ACCEPTABLE USE POLICY

# NASSTAR

## Contents

1	How this Acceptable Use Policy Works.....	3
2	Customer Obligations.....	3
3	Nasstar Rights.....	5
4	Definitions .....	5

## 1 How this Acceptable Use Policy Works

- 1.1 This Acceptable Use Policy (**Policy**) is referred to in Nasstar's General Terms and sets out Nasstar's expectations with regards to the Customer's use of the Services and the communications network over which these are provided.
- 1.2 Breaches or lack of adherence to any applicable clauses contained in this Policy will be seen as a material breach of the Customer's Contract with Nasstar and may ultimately lead to termination of the Contract.
- 1.3 The Customer is responsible for violations of this Policy by anyone using the Services whether authorised by the Customer or not.
- 1.4 The definitions used in this document have the same meanings given to them in Nasstar's General Terms. Any additional definitions, specific to this Policy, are set out the end of this document.
- 1.5 In addition to complying with this Policy, the Customer must also comply with the terms of the Contract. The Customer should note that this Policy is not an exhaustive list of the Customer's obligations in respect of use of Services and the communications network over which these are provided.
- 1.6 Nasstar may update this Policy from time to time and the Customer must at all times comply with the most recent version available on the Website. Continued use of a Service by the Customer will be an acceptance of the Policy as updated.
- 1.7 Nasstar is under no duty, and by this Policy is not deemed to undertake any duty, to monitor or police Customers' activities and Nasstar disclaims any responsibility for any misuse of the Services.

## 2 Customer Obligations

The Services may not be used:

- 2.1 in any way to upload, communicate or otherwise transmit material the Customer does not have any right to;
- 2.2 in any way that breaches any applicable national, federal, state, local or international law or regulation;
- 2.3 in any way to run public internet relay chat services;
- 2.4 in any way which is fraudulent or in bad faith or which, to the Customer's knowledge, has any such purpose or effect and without prejudice to the generality of the foregoing the Services may not be used in any of the following ways or for any of the following purposes:
  - 2.4.1 to perform any activity or conduct that is likely to result in retaliation against, or the interruption, interference, impairment or degradation of, the Nasstar Network or Nasstar Services or which would cause Nasstar to breach the terms of any of its licences or in Nasstar's opinion is likely to be detrimental to Nasstar's business and/or its reputation;

- 2.4.2 in any way that, in Nasstar's reasonable opinion, could or does detrimentally affect the performance of the Nasstar Network, Services, any third party's system or network or that detrimentally affects the quality of Nasstar Services for another customer;
- 2.4.3 to obtain or attempt to obtain unauthorised access to or use of data, services, systems or networks, internet accounts or computers, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication;
- 2.4.4 to monitor and/or transmit data or traffic on any network or system, or to distribute software with such capabilities, without the authorisation of the owner of the system or network;
- 2.4.5 to interfere with a service to any user, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks;
- 2.4.6 to collect information by deceit, including but not limited to internet scamming, password robbery, phishing, security hole scanning and port scanning;
- 2.4.7 using any false, misleading or deceptive TCP-IP\* packet header or any part of the header information in an e-mail or a newsgroup posting;
- 2.4.8 to publish or transmit material that can be interpreted as defamatory, obscene, offensive, inflammatory, infringing any intellectual property rights, being likely to deceive any person or to misrepresent a User's identity or affiliation with any person or organisation, promoting or assisting any illegal activity, being threatening, abusive or invading another's privacy, causing annoyance, inconvenience or needless anxiety;
- 2.4.9 in any way which is in breach any of the IFFOR policies or registering an abusive string in the sTLD;
- 2.4.10 to publish or otherwise distribute Warez, illegal material, software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of the Nasstar Network or a third-party network or participating in any file-sharing/peer-to-peer activities;
- 2.4.11 to generate, or allowing others to generate, calls, emails or data activity causing Nuisance Calls, AIT, SPAM or UCE (unless permitted by law), DDoS or otherwise adversely affecting platform performance;
- 2.4.12 using excessive amounts of server resources as compared to the amount stated within the Contract. These include bandwidth, processor utilisation and/or disk space; or
- 2.4.13 to send, knowingly receive, upload, download, use or reuse material which constitutes or encourages harming children, child pornography, is pornographic, abusive, likely to cause harassment, offensive, indecent, defamatory, sexually explicit, obscene, morally repugnant, excessively violent, incites violence, threatens violence, contains hate speech, creates a risk to public health and safety, compromises national security, is menacing or in breach of any confidence, or which compromises privacy, intellectual property rights or other rights. Nasstar reserves the right to archive any content which

it does not believe to be necessary for the normal operation of the Service, and the definition of this is entirely at Nasstar's discretion.

## 2.5 The Customer must also ensure that:

- 2.5.1 its usage (where applicable) complies with policies of any internet registry or registrar, including RIPE policies as updated and amended on the RIPE website at [www.ripe.net](http://www.ripe.net) from time to time;
- 2.5.2 its usage complies with the rules and conventions for postings to any social media, bulletin board, chat group or other forum in which it participates;
- 2.5.3 its usage complies with all industry guidance, and conditions imposed by the third-party suppliers or operators, relating to the Services and the marketing and advertising of any services it offers;
- 2.5.4 it takes all reasonable steps to ensure that any third-party software, hardware or equipment used with or in conjunction with the Services is not infected by viruses and/or logic bombs, worms, trojan horses and any other type of disruptive, destructive or nuisance programs;
- 2.5.5 it does not make or permit any modifications to any Service without Nasstar's prior written consent; and
- 2.5.6 it promptly renumbers any IP addresses issued to the Customer as part of the Services where required by Nasstar due to technical or other reasons.

## 3 Nasstar Rights

If Nasstar considers that the Customer is using the Services or permitting the Services to be used in breach of this Policy, then Nasstar may take such action as Nasstar considers appropriate which may include:

- 3.1 terminating/suspending all or part of the Services with immediate effect;
- 3.2 taking down or otherwise removing and destroying any materials; or
- 3.3 informing appropriate governmental authorities or other third parties.

For the avoidance of doubt, Nasstar is only bound to manage any Services being provided by Nasstar or to monitor usage where such activities expressly form part of Nasstar's Contract with the Customer.

## 4 Definitions

**AIT (Artificial Inflation of Traffic):** where the flow of calls to a Revenue Share Service (which shall include services to the 070, 084, 087, 090, 091, 098 and 118 number ranges and any other number ranges notified to the Customer in writing) or other equivalent revenue share type services, is disproportionate to the flow of calls which would be expected from good faith usage or an acceptable and reasonable commercial practice relating to the operation use of such service or of telecommunication systems;

**Call:** a signal, message or communication which can be silent, visual or spoken;

**DDoS (Distributed Denial of Service):** an attempt to temporarily or indefinitely interrupt or suspend services connected to the Internet by saturating the target service/platform with external communications requests;

**IFFOR:** International Foundation for Online Responsibility, the policy making body for the .xxx sTLD;

**Nuisance Call:** an unwanted Call which causes annoyance to the receiver of the Call and/or is a hoax Call, and/or is of an offensive, spiteful, abusive, indecent, defamatory, obscene or menacing nature including unauthorised or "spam" Calls and "silent" Calls as defined by Ofcom in its "Statement of policy on the persistent misuse of an electronic communications service" published 20 December 2016, and any subsequent update;

**Revenue Share Service:** a service where an element of the revenue for the Call passed on from the originating communications provider is shared (directly or indirectly) by the communications provider receiving (via a third party in a transit situation) such revenue with the person operating the service (which for the avoidance of doubt may be the communications provider receiving such revenue);

**RIPE:** the Réseaux IP Européens Network Coordination Centre (RIPE NCC) is one of five Regional Internet Registries (RIRs) providing Internet resource allocations, registration services and coordination activities which support the operation of the Internet globally;

**UCE (SPAM or Unsolicited Commercial E-mail):** unsolicited nearly identical messages sent to numerous recipients by email often containing links to phishing websites or malware. Also described as Unsolicited Bulk E-mail (UBE);

**WAREZ:** unsolicited nearly identical messages sent to numerous recipients by email often containing links to phishing websites or malware. Also described as Unsolicited Bulk E-mail (UBE).