An **Acceptable Use Policy (AUP)** is a set of rules and conditions systematized by a network, system or a website owner that define and restrict the ways in which the network, system or website may be utilized.

The **AUP of DATACENTER.BG LLC** is aimed at explicitly outlining the purposes for which customers CANNOT use our hosting services and position data on our network servers.

This Acceptable Use Policy (AUP) is accepted as part of the Dedicated Servers Terms of Service each user agrees to abide by when signing up for a Dedicated server account with our hosting services. Any violation of these AUP terms will be considered as violation of our Dedicated Terms of Service.

We - DATACENTER.BG LLC, shall be the final part to determine whether an act constitutes a violation of this AUP and misuse of our services. We reserve our right to respond accordingly and/or immediately terminate the provision of the services, shall we become aware, and/or have sufficient evidence, of any prohibited conduct outlined in this AUP, or any other action threatening the secure environment of our hosting customers and/or network of servers. We shall be the sole arbiter in determining the sufficiency of the present evidences.

In order to protect our company's reputation and responsibilities, and guarantee robust and reliable hosting service to all our customers, as well as the privacy and security of all our individual users, we - DATACENTER.BG LLC - hereby state the following AUP conditions to come into force for each user signing up for a Dedicated server hosting account with our hosting services:

- ## COMPLIANCE WITH LAW

  The Customer shall not post, transmit, re-transmit or store material on or through any of the Services or Products which, in the sole judgment of the Company (i) is in violation of any local, state, national or non-Bulgarian law or regulation, (ii) threatening, obscene, indecent, defamatory or that otherwise could adversely affect any individual, group or entity (collectively, "Persons") or (iii) violates the rights of any person, including rights protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Customer. The Customer shall be responsible for determining what laws or regulations are applicable to the use of the Services and Products.

- ## CUSTOMER SECURITY OBLIGATION

  Each Customer must take a reasonable care of keeping each server or network device attached to the Company's infrastructure up-to-date and patched with the latest security updates. Failure to protect a server may result in a security compromise by outside sources. The Company is not responsible for Customer server level security unless a security administration package, a firewall security administration package or a fully managed operating system package is contracted for and maintained. A compromised server creating network interference will result

in immediate Customer notification and will be disconnected from the network immediately so as to not directly affect other Customers. No service credits will be issued for outages resulting from disconnection due directly to breached server security. The Customer is solely responsible for any breaches of security affecting servers under Customer control, including repairing the system, terminating the account(s) of the abusive user(s), and reporting occurrence of the issue to abuse@datacenter.bg. If a Customer intentionally creates a security breach, the cost to resolve any damage to the Customer's server or other servers will be charged directly to the Customer. The labor used to resolve such damage is categorized as emergency security breach recovery and is currently charged at 90.00 EUR per hour.

- # SYSTEM ABUSE

Any Dedicated server hosting customer in violation of our system or network security will be subject to criminal and civil liability, as well as immediate account termination. Examples include, but are not limited to the following:

- Unauthorized access, use, probe, or scan of our system's security, authentication measures, data or traffic. Interference with the service to any user, host or network including, but not limited to: e-mail bombing, flooding, deliberate attempts to overload the system and broadcast attacks, forging of any TCP/IP packet header or any part of the header information in an e-mail or newsgroup posting.
- Any attempt at doing harm to a server or a customer of DATACENTER.BG LLC services:

  DATACENTER.BG LLC will immediately and resolutely react to any attempt at misuse of an Internet account or computer, or any attempt to gain access to an internet account or computer by a Dedicated server hosting customer unauthorized by the account/computer owner. Such attempts include, but are not limited to the following: 'Internet scamming' (tricking other people into releasing their passwords, etc.), password robbery, security hole scanning, running proxy - proxy lists and any kind of proxy scripts (including, but not limited to php proxy and nph proxy), introducing of any computer programs (viruses, Trojan horses, trap doors, back doors, worms, time bombs, packet bombs, cancel bots, etc.) that are intended to negatively interfere with, intercept, irreversibly damage or take hold of any system, data or personal information. It WILL NOT matter whether the attacked account or computer belongs or not to DATACENTER.BG LLC services. The fraud will be subject to actions based on the very nature of the attack and those may represent a warning, an account suspension or cancellation, and/or civil or criminal legal actions.

- Executing any form of network activity that will intercept data not intended for the Customer's server.

- Interfering with or denying service to any user, host, or network other than the Customer's host (example: denial of service attack or distributed denial of service attack).
- Conduct designed to avoid restrictions or access limits to specific services, hosts, or networks, including but not limited to the forging of packet headers ('spoofing') or other identification information.
- Failing to comply with the Company's procedure relating to the activities of the Customers on the Company's premises. Violators of the policy are responsible, without limitations, for the cost of labor to correct all damage done to the operation of the network and business operations supported by the network. Such labor is categorized as an emergency security breach recovery and is currently charged at $100.00 USD per hour required. Network interference by any Customers that may cause or is currently causing network interference with another Customer will be disconnected immediately. No service credits will be issued to Customers disconnected for network violations.

• EMAIL POLICIES

SPAMMING IS PROHIBITED. Users MAY NOT utilize our Dedicated server hosting services to transmit, distribute or deliver any unsolicited bulk or commercial messages over the Internet (an action known as "spam" or "spamming"). Users MAY NOT utilize our dedicated servers for email marketing purposes. There is a 500-outbound-email-per-hour limit on all dedicated servers.

Spamming is a violation of ethic norms and will be interpreted as an infringement. DATACENTER.BG LLC will not tolerate the sending of unsolicited bulk or commercial messages through our Dedicated server hosting services, as well as through another service that is mentioning, in some way, our customer's domain name or implies the utilization of our server network or our e-mail services for sending the unsolicited bulk or messages.

SPAMVERTISING IS PROHIBITED. 'spamvertizing' refers to the practice of sending unsolicited spam messages for the purpose of advertising a particular website.

If such e-mails are relayed through 3rd party (e-mail spoofing) and/or are promoting a domain hosted on our servers, this will lead to immediate account suspension unless an evidence of legitimacy for non-involvement of the domain owner in the particular illegal action is provided.

'E-mail spoofing' is a fraudulent e-mail activity in which the sender's (3td party) e-mail address and other parts of the e-mail header are changed so as to appear that the e-mail has been sent from a different source (e-mail address owner/server).

'Unsolicited message' is a message that is sent against the privacy policy of a newsgroup, or is sent to a recipient without their explicit permission. We, at our sole discretion, shall determine whether any of the messages you are sending is spam or spamvertizing. For your information, spamming generally includes, but is not limited to the following

- Sending of unsolicited messages in bulk, or sending of unsolicited e-mails, which provoke complaints from recipients;
- Sending of junk mail;
- Use of distribution lists that include people who have not given prior explicit permission to be involved in such a distribution process;
- Posting commercial ads to USENET newsgroups that do not permit it;
- Posting articles containing binary encoded data to non-binary newsgroups;
- Excessive and repeated posting of off-topic messages to newsgroups;
- Excessive and repeated cross-posting;
- E-mail harassment of another Internet Customer or Customers, including but not limited to, transmitting of any threatening, libellous or obscene material, or material of any nature that may be deemed offensive;
- E-mailing of age-inappropriate communications or content to anyone under the age of 18.

BLOCK REMOVAL: If Customer actions have caused Company mail servers or Company IP address ranges to be placed on black hole lists and other mail filtering software systems used by companies on the Internet, the Customer will incur a 100 EUR charge to the Customer's account and 100 EUR per hour for administrative charges incurred to remove and protect mail servers and IP ranges.

- Drop-Box Accounts. Using this network for the receipt of replies to unsolicited mass email (spam) sent from a third-party network is prohibited.
- Header Forgery: Forgery of email headers ('spoofing') is prohibited.
- Proxy Spamming: Spamming via third-party proxy, aggregation of proxy lists, or installation of proxy mailing software is prohibited.
- Relaying. Configuration of a mail server to accept and process third-party messages for sending without user identification and authentication is prohibited.

MASS MAILINGS: Sending mass unsolicited email is considered spam. Unsolicited email is defined as email sent to a recipient who has not double-opted in to mailings from the Customer. Senders of mass mailings must maintain complete and accurate records of all opt-ins, including the email and its headers if applicable, and provide such records to the Company upon request. If positive and verifiable proof of opt-in cannot be provided, complaints from recipients of the mailing are considered proof they did not subscribe and the mailing is unsolicited.

MAILING LISTS: Company's mass mailing rules also apply to mailing lists, list serves, or mailing services contracted for by the Customer. The policy is stated as follows: An acceptable mailing list will be focused at a targeted audience that has voluntarily signed up for e-mail information using a double opt-in process or that has made their e-mail address available to the Customer for distribution of information. The list must also allow for automatic removal by all end Customers with non-distribution in the future

- # IP ALLOCATION

The Company administers an Internet network on which multiple Customer servers reside. Customers shall NOT use IP addresses that were not assigned to them by the NOC staff or network administrators. Any server utilizing IP addresses outside of the assigned range will be suspended from network access until the IP addresses overlap can be corrected. Use of an unauthorized IP address will result in a charge of 50 EUR per IP. Use of an unauthorized IP address creating a third party Customer outage will result in a 200 EUR charge and termination of service until the IP allocation is resolved.

- # IRC POLICY

The Company allows stand alone IRC servers which are not connected to global IRC networks such as Undernet, EFnet, DALnet and other IRC networks. IRC servers which establish and maintain connections to global IRC networks such as Undernet, EFnet, DALnet and others will be considered to be in violation of the Acceptable Use Policy.

The Company does not allow IRC plug-ins, scripts, add-ons, clones or other software that has the intent or effect of disrupting or denying service to other users. Harassing, disrupting or denying service to other users is expressly prohibited, and may result in the immediate suspension or cancellation of Customer account(s).

If IRC servers attract DoS or DDoS attacks that disrupt or deny service to other Customers, the Company will null-route, ACL or otherwise suspend service to maintain quality of service for other Customers on our network.

The Company allows the limited use of stand-alone IRC 'bots'. The Company prohibits the use of 'botnets'. A Customer's IRC server may run a 'bot', but the Customer may not join a 'botnet'. The use of IRC BNC's or other proxy and re-direction software is expressly prohibited.

For the purposes of policy enforcement, any malicious activity observed to originate from a Customer's server may result in the immediate suspension of service to the offending Customer's server without prior notice. Frequently compromised servers may be reviewed for account termination on a case-by-case basis. The purpose of this case-by-case review is to deter AUP prohibited activity from occurring under the blanket excuse of a 'compromised server.'

Harassing, abusive and aggressive IRC activity is prohibited. This includes 'flooding' (rapid transmission of information with the intent to harass or deny service), 'hijacking' (taking improper or unauthorized control of B channel or server operator privileges), sending messages to users who do not want them, attempting to circumvent a channel or server ban, impersonating other IRC users and other abusive IRC behavior as determined by the Company.

The Company reserves the right to modify or amend the IRC policy at any time.

• INAPPROPRIATE OR UNLAWFUL CONTENT

CONTENT published or transmitted via DATACENTER.BG LLC's Dedicated servers includes website content, email content, forum/blog postings, chat content, and/or any other type of content hosted on our Dedicated servers, published online or transmitted through our network's services.

The user of our Dedicated server hosting services is NOT permitted to post online content or have links to content that:

- is defamatory, abusive or obscene, violates a person's reputation/privacy, is reasonably deemed offensive by the web community, is anti-religious or anti-human rights, or contains any type of threatening or hate speech, encourages harassment or physical harm to any group or individual, or is otherwise malicious/fraudulent and may result in complaints/liabilities/or retaliation against DATACENTER.BG LLC by offended viewers;
- promotes or encourages illegal activities (e.g. illegal drugs, illegal gambling, arms trafficking, etc.) or violates any applicable law, statute, ordinance or regulation, including but not limited to the laws and regulations governing export control, unfair competition, false advertising, consumer protection, etc.
- represents pornography - any type of pornographic/adult material, including child pornography, or advertisements of pornographic websites;
- represents infringement on copyright, patents, trademarks, trade secrets, or third party's intellectual property or proprietary rights, including pirated computer programs, hacking/phreaking software, warez or any type of software/content (including also ROMs, ROM Emulators, media files - MP3, AVI, .RM, etc., torrent files, and others) that is copyrighted, is NOT uploaded in compliance with its license agreement or is NOT freely available for distribution.

• COPYRIGHTS

Copyrighted material must not be placed on customers' Dedicated server hosting accounts without the explicit permission of the copyright owner or a person specifically authorized to give such permission by the copyright owner. Upon receipt of a claim for copyright infringement, or a notice of such violation, we will immediately run full investigation and, upon confirmation, will promptly remove the infringing material from the Services. Further procedures (in accordance with our stated below corrective measures) will be carried out if necessary. We will assume no liability to any customer of the Dedicated server hosting services for the removal of any such material. Repeated violations of PublicDomainRegistry's Copyright Infringement Policy could result in permanent suspension of a customer's account.

- # **CORRECTIVE ACTIONS**

We reserve our right to be the sole arbiter in determining the seriousness of each infringement and to immediately take corrective actions.

We will disable the customer's Dedicated server hosting account if we deem necessary, at our sole discretion. Upon closing of the customer's account we will send an e-mail notification to the customer, stating the reason for the termination and quoting our terms' chapter that has been violated. The customer will be given an opportunity to respond and take measures to remedy the situation should he/she consider him/herself abused by a third party. Upon fulfilling of this obligation, we may re-activate the customer's account, if we find, at our own discretion, sufficient evidence pro customer's side.

Closed accounts due to repeated violations will not be re-activated.

- # **REPORTING VIOLATIONS**

If you need to report a violation of this AUP agreement or believe that you or your system has been subject to attack originating from our system, please contact us immediately. Our team will fully investigate the situation and provide you with professional assistance.

- # **POLICY FOR HOSTING RESELLERS**

If you are using your dedicated server for reseller hosting purposes, you are responsible for the conduct of your Customers and by agreeing with this AUP, agree that your Customers will adhere to the AUP. Hosting resellers should make their perspective Customers aware of the AUP and the consequences for violation.

- # **REVISIONS**

We reserve our right to change this AUP at any time, without prior notice. We encourage our users to periodically review this Acceptable Use Policy and our Dedicated Servers Terms of Service.