DDOS-GUARD

Acceptable
use policy

IQWeb FZ-LLC

IQWeb FZ-LLC is a legal entity and managing company operating under well-known brand name DDoS-Guard

+55 613 550-74-40
+31 970 1028-0960
+971 58 506-81-27

sales@ddos-guard.net

Table of contents

1. General terms

Revision date and effective date — 13.01.2025

1.1. This Acceptable use policy (hereinafter referred to as the "Policy") defines the limits of permissible use services established by IQWeb FZ-LLC (hereinafter referred toas the "Provider") to any persons, including, but not limited to legal entities and individuals (hereinafter referred to as the "Client").

1.2. This Policy is an integral part of the Service Level Agreement posted at the following Internet link — https://ddos-guard.net/file/sladdg_en.pdf

1.3. The Client's use the Company's services is the Client's full and unconditional acceptance of the terms of this Policy.

2. Prohibited ways of using the services

2.1. The Client undertakes to use the Provider's Services without violating the law and only for legitimate purposes, as well as to prevent abuse of them. The use of the Services in violation of the provisions of the current legislation is prohibited.

2.2. Illegal use includes, but is not limited to, the following types of actions:

2.2.1. Trafficking in prohibited items and materials, drug trafficking;

2.2.2. Threat of bodily injury or damage to individuals or groups of persons, harassment;

2.2.3. Sending messages of an obscene or offensive nature, as well as messages intended to threaten or harass a person;

2.2.4. Fraud schemes, gambling, piracy (distribution of copyrighted materials in violation of copyright law);

2.2.5. Using by the Client or the Client's end user of the domain name (including redirection to websites) for the purpose of creating, transmitting, distributing or storing materials, information and methods, or performing actions that violate the rights to trademarks, patents, copyrights, trade secrets, or rights to other intellectual property objects;

2.2.6. Using by the Client or the Client's end user of the domain name (including redirection to websites) for the purpose of creating, transmitting, distributing or storing materials, information and methods, or performing actions that violate the confidentiality of personal data, public and other personal rights of third parties; use tools designed to violate security (including password recovery software, hacking tools, or other network scanning tools);

2.2.7. Using by the Client or the Client's end user of the domain name (including redirection to websites) for the purpose of creating, transmitting, distributing or storing materials, information and methods, or performing actions that: violate international export control, information protection or anti-terrorist laws; violate banking secrecy; violate the secrecy of communication, whether it is vulgar content, threats, blackmail, discrimination, violence or incitement with malicious intent, against a certain group of people; use tools for the purpose of insulting; use content that knowingly contains viruses, or content that provokes any crimes or civil unrest;

2.2.8. Using by the Client or the end user of the domain Client to distribute a large number of materials of exactly the same content or sending them to thematic conferences in the form of spam messages, sending a large number of emails to persons who did not express a desire to receive them, regardless of whether this mailing provoked complaints from recipients, whether there was the presence of falsified headers and false contact information, sending broadcast messages or any messages sent in a way that has an intrusive nature, regardless of the location of the recipients (the Provider adheres to a policy that does not allow sending spam messages, offensive messages and messages containing advertising to persons who have not expressed a desire to receive them);

2.2.9. An attempt to gain access to a computer system without the permission of the copyright holder, any attempt by the Client or the Client's end user to hack, manipulate, persuade, assist or facilitate the manipulation or hacking of the security modules of the Provider's network or any other of its systems (including for the purpose of obtaining unauthorized access to information or using information, system or network; scanning or testing of a system or network for vulnerabilities; violations of security measures; unauthorized monitoring of information or traffic; preventing the normal provision of services to any client, host or network; substitution of any TCP/IP protocol headers for packets and any other part of the message header);

2.2.10. Initiating, facilitating, instigating or using the domain name or URL of the Client or the Client's end user to direct or redirect any malicious traffic, denial of service attacks (DOS and DDoS attacks or);

2.2.11. Attempts to circumvent any user authentication or security of the host, network, or account, actions aimed at obtaining unauthorized access to data not intended for the user by services and services (Client);

2.2.12. Stress tests and security checks, including: port scanning, ping flood, packet substitution and forgery of route information;

2.2.13. The creation of code to carry out malicious effects on third-party computers, the spread of viruses and (or) in IRC bots, the use or distribution of software created to disrupt the functioning of the security system or containing computer viruses or Trojan programs. Examples of such software include, but are not limited to the following types: password matching programs, password crackers or network scanning tools, cryptographers;

2.2.14. Using the Provider's Services in order to disrupt the functioning of the security system of system resources or accounts (accounts) on the Provider's servers and resources or any other websites;

2.2.15. Using the Provider's Services to ensure the functioning of the cryptocurrency, including for its generation and (or) storage and (or) mining (mining) using specialized software or in any other way;

2.2.16. Violation of any customs and export restrictions;

2.2.17. Any other violation of the law.

2.3. The Provider has the right to determine the lists of domains in respect of which services and Services cannot be provided, possible and impossible adjustments to the parameters of Services and other acceptable criteria related to the provision of Services. The Provider has the right to change the above parameters and lists at any time, introduce new criteria or remove previously existing ones. The reason for the domain being in the list of unavailable Services can be clarified by contacting the ticket system within the Client's Personal Account on the Provider's official website.

2.4. When using the Provider's Services, it is prohibited to carry out excessive consumption (overload) of computing resources of the server/s or the Provider's equipment, including, but not excluding, dedicated servers, VDS (virtual dedicated servers), hosting capacities and other equipment, due to the possible negative impact on other Clients and on equipment and infrastructure companies. The degree of permissible consumption of computing resources (including the degree of maximum utilization and the permissible time of use in maximum utilization mode) is determined by the Provider at its discretion. The Client undertakes to eliminate excessive consumption (overload) of resources at the first request of the Provider in the appropriate time.

2.5. If the Client is involved in a violation of the functioning of the security system, the Provider reserves the right to disclose to the system administrators of third-party websites the account names of all users involved in such violations in order to assist in suppressing cases of creating a security threat.

3. Prohibited ways of using the materials

3.1. The Client is responsible for any information accessed through the use of services provided by the Provider, regardless of whether it is made with the knowledge and consent of the Client or without it.

3.2. Materials in the public domain (for example, images, texts and programs) can be downloaded or downloaded from resources using the Provider's Services. Clients have the right to post materials on their resources, providing free public access to them. At the same time, the Client assumes all risks associated with the publication of materials in the public domain.

3.3. The Client is prohibited from storing, distributing or transmitting prohibited materials using our services. Prohibited materials include, but are not limited to the following types:

3.3.1. Containing threats of physical harm, violent scenes provoking violence, or containing offensive or hateful statements;

3.3.2. Infringing copyrights containing trademarks and other patented designations used without appropriate permission, as well as intended to assist others in overcoming technical means of copyright protection;

3.3.3. Clearly infringing the rights to other persons' trademarks and commercial service marks, patents or other proprietary rights;

3.3.4. Containing false or misleading information that violates consumer protection laws of any jurisdiction, including information about financial chains and pyramids;

3.3.5. Discrediting or violating the boundaries of a person's private life;

3.3.6. Creating a risk to the safety or health of people, public safety, endangering national security or hindering the investigation by law enforcement agencies;

3.3.7. Unlawfully disclosing commercial secrets or other confidential information of any person protected by law;

3.3.8. Promoting drug trafficking, violating export and customs control laws related to illegal gambling or illegal arms trafficking;

3.3.9. Promoting the spread of terrorism and inciting any ethnic, social or religious discord;

3.3.10. Propagandizing and promoting the spread of child pornography.

3.3.11. Posting or displaying any images or wording related to incest, bestiality and other similar content anywhere on the site, including URLs and meta tags;

3.3.12. Extorting funds for purposes prohibited by the legislation of the countries where the Provider and the Client are located;

3.3.13. Containing other illegal information of any kind that offends the feelings of users.

4. Mass or commercial mailing by the e-mail

4.1. The Client is obliged to comply with the anti-spam legislation and any other laws or requirements of international organizations regulating the procedures for mass mailing of e-mail messages.

4.2. In addition, for each mass mailing, the Client must obtain the prior approval of the Provider. Such approval cannot be given if the Client is unable to provide all of the following confirmations for sufficient compliance with the Provider's requirements:

4.2.1. The intended recipients of the Client's mailing list have given their consent to receive the e-mailing using such confirming means as subscription to the newsletter;

4.2.2. Consent procedures include the necessary measures to ensure that the person who gave his consent was the owner of the email address to which consent was given to receive the newsletter;

4.2.3. The Client retains proof of consent in a form that can be provided immediately upon request, and also provides the possibility of providing confirmation of consent at the request of the recipients or the Provider within 72 hours after receiving the request;

4.2.4. The Client has tools that allow the recipient to withdraw his consent without hindrance — for example, in the form of a link in a letter or instructions in a response with the word "Unsubscribe" in the subject line. The withdrawal of consent is carried out within 72 hours, and the Client must notify the recipients that the withdrawal of consent will be carried out within 72 hours;

4.2.5. The Client must publish an email address for complaints (for example, abuse@yourdomain.com) in a prominent place on any website associated with e-mail, and the Client must register this address on abuse.net and promptly respond to messages sent to this address;

4.2.6. The Client must have published a Privacy Policy (regarding the processing of personal data) for each domain associated with the e-mail newsletter;

4.2.7. The Client has the ability to track anonymous complaints;

4.2.8. The Client cannot hide the source of the Client's email in any way. The Client's email address must include the email addresses of the recipients in the email or in the "TO" line of the email.

These rules apply to messages sent using the Provider's Services or to messages sent from any network by the Client or any person on behalf of the Client who directly or indirectly point the recipient to the website or email address posted using the Provider's Services.

4.3. The Client cannot use the e-mail service provided by a third-party company that does not practice similar procedures for all its clients. The Provider has the right to check or otherwise monitor the Client's compliance with these requirements and may block the sending of e-mail that violates these terms.

4.4. The Client may not use the Provider's mail services, servers or equipment to send advertisements to other websites that are not related to the Client's website.

5. Violation of the Terms

5.1. Violation of the Policy entails criminal, administrative or civil liability.

5.2. The Provider supports the principle of freedom of speech on the Internet and will not suspend or disable the Service to the Client just because we or someone does not agree with the opinion expressed on the Client's website. However, where there is reason to believe that the Client's online activity violated the legitimate rights and interests of a third party, the Provider reserves the right, at its discretion, to determine what actions, including, but not excluding, termination of the provision of Services, will be taken in respect of each specific case.

5.3. If the Provider becomes aware of possible cases of violation of the Policy, the Provider has the right to initiate an investigation procedure, which may include the collection and analysis of available information about the Client and the Services used, as well as information from the applicant who filed the complaint, if any, as well as the study of data available to the Provider. The Provider, at its discretion, determines exactly what actions will be taken in relation to each specific case, taking into account its individual characteristics.

5.4. Complaints about abuse, violation and misuse of the Services described in this Policy may be sent by applicants in the form of a written document to the following postal address: Office No 122, dic Building 03, Dubai or by sending signed document to the email address: abuse@ddos-guard.net

5.5. The complaint must contain:

5.5.1. If the applicant is an individual - surname, first name, patronymic, passport data, residence address (correspondence address), a duly certified copy of the applicant's passport; if the applicant is a legal entity — the full name of the legal entity, TIN and OGRN of the legal entity, legal address, documents confirming the authority of the person acting on behalf of legal name without power of attorney;

5.5.2. Data on the authorized person equivalent to clause 5.6.1. and a power of attorney, if the applicant acts on the basis of a power of attorney.

5.5.3. Consent to the processing of personal data for the purposes of resolving the complaint, including the transfer of them to third parties;

5.5.4. Court decision or resolution of the relevant state body.

5.6. The complaint may not be accepted for consideration if it does not contain the conditions specified in clauses 5.4. and 5.5 of the Policy.

5.7. Any person filing a false complaint or a complaint containing misleading information must compensate the Provider for any damage caused as a result of filing such a complaint.

5.8. The Provider may offer end-to-end solutions for network services exclusively for traffic filtering (without physically placing any data on the Provider's facilities), which are associated with the change of DNS A-records and relevant information in WHOIS services. To clarify the data on the placement of the network service, you must contact the owner of the network service (website / server) directly.

5.9. By agreeing to this Policy, the Client refuses and undertakes to protect the Provider from any claims related to any actions taken by the Provider as a stage of verification of an alleged violation of this Policy or the result of the conclusion that a violation has been committed. The Client cannot file a claim or seek compensation for any losses incurred as a result of the Provider's decision to remove material from its servers, issue a warning to the Client, suspend or close his account, as well as perform any other action during the verification of the alleged violation or on the basis of the conclusion made by the Provider that the violation was admitted. This disclaimer applies to all violations described in the Policy.

6. Changes in the Policy

6.1. The current version of the Acceptable use Policy is always available at the following Internet link: https://ddos-guard.net/file/AUP.en.pdf

6.2. The Provider has the right to make changes to this Policy (publish a new version) without any special notification to the Client and (or) third parties, while the new version of the Policy comes into force from the moment it is posted on the Internet on the Provider's website. The Client's use of the Services after the date of entry into force of the new version of the Policy means that the Client accepts the changes made by the new version in full. In case of disagreement with the new version of the Policy, the Client is obliged to stop using the Services.

6.3. For questions related to the implementation of the procedures and requirements specified in the Policy, it is possible to contact the postal address: Office No 122, dic Building 03, Dubai, or by sending signed document to the email address: abuse@ddos-guard.net.