Service Abuse and Acceptable Use
By using our services, you agree to not abuse systems or networks in any way that may harm the usability of other client services or harm outside networks or individuals. We have a zero-tolerance policy for abuse. We also work with security organizations in order to deal with abuse cases accordingly. Below is a non-exclusive list of actions considered abusive, but is not limited to. Any doubt should be referred to our abuse department for evaluation.

Actions considered abusive, but not limited to:
1. Host or distribute malicious or inappropriate files.
2. Targeted harassment towards individuals (invasion of privacy) (“DoXing”), retaining any personal information against them without their consent. This may also include hateful and/or racist content or any type of discrimination.
3. Carry outbound network attacks (DoS), malicious network scanning or host malware (e.g botnet).
4. Host, share or use anything copyrighted, illegal or cracked without the permission of the owner, including server license cracking (e.g TeamSpeak servers, forum software, etc.).
5. Host ToR exit nodes.
6. Host fraud, phishing, gambling/lottery sites or software.
7. Send unsolicited e-mail spam.
8. Host any kind of nudity, abusive, pornographic, offensive, illegal, or inappropriate, controversial, racist, violent, sexually explicit, erotic, extremist or drug content.
9. Use the services for any abusive activities on the internet.
10. Host a VPN as they are usually the reason behind most of the DMCA notices and abuse. Using our services to protect yourself while gaming is prohibited.
11. Host anything that’d attract network attacks that are not officially supported (e.g VPN) or attack our network intentionally. Please open a ticket if you are unsure whether we can protect your application or not. We reserve the right to suspend anything that attracts attacks and causes disruptions to our network.
12. Usage of any forms of resource abuse that may cause harm to other clients (e.g cryptocurrency mining).
13. Set rDNS to something which promotes illegal activities such as hacking, DDoS, drugs or anything inappropriate.
14. Utilize 100% of allocated cores for an extended period of time on a shared service (Virtual Private Server (VPS), Virtual Dedicated Server (VDS), Game Hosting. If you run software that requires high CPU usage on a constant or unusual basis, please contact us beforehand.

Doing anything of that may lead to the suspension of your service or your account being terminated along with all services associated with it depending on the severity. Repeated violations will result in all services associated with your account being terminated without prior notice. You, the customer, are fully responsible for your servers. If you’re reselling our products, you will be held accountable for any violation of our terms.

Bandwidth Fair Use
Overloading the network and inconvenience to other customers may be caused by individual users who use much more traffic than the average of similar customers.

We reserve the right to monitor the amount of data traffic and filter excesses. Under normal circumstances, there is no overage of data traffic. If the amount of data traffic differs significantly from the average, we will contact the customer about how to normalize the usage. If the customer does not normalize his consumption, we can block (temporarily) data traffic or charge the customer.

Data Responsibility
The client is responsible for his/her own data. We are not responsible for any data, nor anything that could happen to the server. We are not required to provide any backup in case of data loss. Backup the data on a daily basis for all the servers as we are not bound to provide any data backup. We will not be held responsible for the loss of data in case of any failure.