



Acceptable Use Policy

Article 1. Definitions

Network: Data communication network and/or infrastructure over which the Supplier provides the Services to the Client.

User: The natural person who has an authorization from the Customer for the use of the Network, Systems and Services.

Usage limits: the limits set by Supplier on capacity (e.g. the amount of data traffic, processing capacity, memory, storage or power) that Customer may or may actually use under the Agreement.

Systems: computer and related equipment of the Supplier with which the Supplier grants the Customer access to the internet.

Article 2. General

This Acceptable Use Policy (hereinafter referred to as: "AUP") of the Supplier applies to the Customer's use of the Service(s) and Network of the Supplier. The purpose of the AUP is to assist Customer in the responsible use of the Network and Services, and to avoid practices that reduce/affect the usability and performance of the Network and Services.

The terms used and defined in the Supplier's General Terms and Conditions retain their meaning in this AUP, unless expressly deviated from in this AUP. Customer undertakes to comply with this AUP for acceptable use at all times, and upon Supplier's request, Customer shall confirm compliance.

Article 3. Acceptable Use

Customer is permitted to use the Services for any activity permitted by law in accordance with the Agreement. Customer shall instruct its Users to comply with the AUP.

Customer will:

- A. ensure that all Accounts that may be used by Customer or Users have a sufficiently strong password;
- B. prevent vulnerabilities in its network and/or systems and immediately repair them;
- C. keep its systems up-to-date through upgrades and updates;
- D. observe and comply with the Supplier's applicable guidelines and procedures with regard to Information Security, and;
- E. investigate, handle and report violations by Customer, Users or third parties to Supplier.

If the Customer finds that this AUP has been violated, it is requested to report this to the Supplier via: **abuse@hypernode.com**.

Article 4. Unacceptable use

Use of the Services and the Network is subject to the condition that the Customer and/or its Users do not use them for illegal or unlawful purposes.

The following types of use or reasonable suspicion thereof by the Customer and/or its Users of the Network and/or the Services shall be considered unacceptable use. Unauthorized use is considered a material breach of the AUP and the Agreement. Customer agrees not to use the Service(s) and the Network to store or distribute data/data that:

1. contain or refer to malicious content (such as viruses, malware or other harmful software);
2. infringe the rights of third parties (such as Intellectual Property Rights), or are manifestly defamatory, harmful, threatening, abusive, discriminatory, hateful or otherwise objectionable;
3. inciting or facilitating criminal or fraudulent conduct;
4. contain hyperlinks, torrents or references with (repositories of) material that infringes intellectual property rights;
5. contain any form of criminal pornography or are apparently intended to help others find such material;
6. constitute a violation of the privacy of third parties, including in any case, but not limited to, the processing of personal data of third parties without consent or any other basis;

7. contain unsolicited, unauthorized or unlawful advertising, promotional materials, spam and junk mail, or;
8. hinder other customers of the Supplier or third parties or cause damage to systems or networks of the Supplier or third parties. The Customer is not permitted to initiate processes or programs that Customer knows or should know are interfering with Supplier or third parties, or that may cause damage.

Article 5. Network

When using the Network, Customer shall have sufficient protective measures in place to scan incoming Internet traffic for malicious content and to be able to take appropriate measures to prevent viruses, including but not limited to, for example, the purchase and installation of the necessary anti-hacking software and virus protection.

Unless expressly agreed otherwise in writing by the Parties, the Supplier is in principle not liable for the content and security of messages sent via the Network and the Services. The Supplier is not under a general obligation to monitor information provided by the Customer that the Supplier passes on or stores in the context of the Services, nor is the Supplier obliged to actively look for facts or circumstances that indicate illegal activities.

Without prejudice to the foregoing, the Supplier has the right to investigate the traffic over its Network and Systems at any time if it deems it reasonably necessary in order to be able to take the necessary measures if necessary. Supplier reserves the right to immediately remove any inappropriate material or data and to block Customer's use of the relevant portion(s) of the Network, if the use or purpose thereof is not in accordance with this AUP.

The Customer and Users must cooperate with the Supplier in the event of any interventions that the Supplier deems necessary to comply with this AUP and in particular to prevent the transfer or storage of illegal information.

Article 6. Shared infrastructure

If no Usage Limits apply to the Services, the Customer shall make use of the Services in an average, reasonable and proportionate manner. As there is a shared infrastructure, Customer's excessive use of the Services may result in congestion of the Network and disruption to other customers. Customer will only use the Services in a way that does not cause inconvenience to other users and does not overload the Network.

In order to prevent excessive use, the Client will, if desired, inform the Supplier in a timely manner as well and completely as possible about its wishes and expectations with regard to

 +31 20 521 6226  support@hypernode.com  Koningstraat 30-1, 6811 DG, Arnhem

usage capacity so that the Supplier can offer the most suitable solution. If, despite this, excessive use occurs, the Supplier will notify the Customer and the Customer will adjust the use to the level advised by the Supplier. If the Customer does not follow such advice from the Supplier, the Supplier may (temporarily) block access to the Network and the Services or charge costs.

Article 7. Digital Services Act, measures and procedures

1. Team.blue nl B.V. ("team.blue") (including its subsidiaries) adheres to the measures set out in the EU Regulation no. 2022/2065 – Digital Services Act ("DSA"). Users are responsible for the content they upload, share, or otherwise make available on our services. Any content that violates the DSA, other applicable law or our Terms & Conditions may be subject to removal, and users may be subject to account suspension or termination on team.blue's initiative.
2. We will cooperate with relevant authorities as required by the relevant regulation and DSA, including providing information (including personal data) and assistance in investigations. The single point of contact will be reachable, at the following email address: **abuse@hypernode.com** (the "Abuse Email").
3. If any person or entity is aware of the presence of specific items of information and/or content on Hypernode's service that individual or entity considers to be illegal content, the individual or entity may contact Hypernode at the Abuse Email and send a report (the "Report") that meets all of the requirements below:
 - a. a sufficiently substantiated explanation of the reasons why the individual or entity alleges the information in question to be illegal content; and
 - b. a clear indication of the exact electronic location of that information, such as the exact URL or URLs, and, where necessary, additional information enabling the identification of the illegal content adapted to the type of content and to the specific type of hosting service; and
 - c. the name and email address of the individual or entity submitting the notice, except in the case of information considered to involve one of the offenses referred to in Articles 3 to 7 of Directive 2011/93/EU; and
 - d. a statement confirming the genuine belief of the individual or entity submitting the notice that the information is accurate and complete.
4. Once Hypernode receives a report, it will send a confirmation receipt to the individual or entity without undue delay. Where a Report meets the above requirements, Hypernode will notify that person or entity of its decision, providing a "statement of reason". Hypernode is not required to undertake a detailed legal examination of the facts in the Report, but must carry out a review at the level expected of a diligent hosting provider.
5. If the individual or entity does not agree with Hypernode's decision, they may contact Hypernode once again, at the Abuse Email, setting out the reasons they do not agree

with the decision. Hypernode will examine the request and communicate the final decision to the individual or entity. Notwithstanding the above process, the individual or entity may also report the allegedly illegal content or activity to public authorities in order to defend its rights.

6. To enhance transparency and in compliance with the DSA, Hypernode may publish reports outlining its content moderation practices, including the number and nature of content removals and user accounts suspended or terminated.

Article 8. Protection

The Supplier may recover the damage resulting from violations of these rules of conduct from Customer. Customer shall indemnify and hold Supplier harmless from (i) claims by third parties in respect of any content or material contained on the Network or Supplier's Systems; (ii) any breach of any applicable law or regulation, and (iii) any breach of this AUP by Customer.