

Abuse & Misbruikbeleid

Laatst bijgewerkt: 16 september 2026

PlayNode wil een veilige, betrouwbare en stabiele hostingomgeving bieden voor alle klanten.

Dit Abuse & Misbruikbeleid beschrijft welk gebruik van de infrastructuur van PlayNode niet is toegestaan, hoe PlayNode omgaat met meldingen van misbruik en welke maatregelen kunnen worden genomen wanneer een dienst wordt misbruikt.

Dit beleid vormt een aanvulling op de **Algemene Voorwaarden**, het **Fair Use / Acceptable Use Policy** en het **Privacybeleid** van PlayNode.

1. Reikwijdte

Dit beleid is van toepassing op alle diensten die door PlayNode worden geleverd, waaronder:

- gamehosting
 - serverhosting
 - VPS-diensten
 - web- en applicatiehosting
 - opslagdiensten
 - netwerkdiensten
 - aanvullende diensten
-

2. Verantwoordelijkheid van de klant

De klant is verantwoordelijk voor het gebruik van zijn account en de aan hem beschikbaar gestelde serveromgeving, voor zover dit volgens de wet aan de klant kan worden toegerekend.

De klant is verantwoordelijk voor:

- de software die op de server wordt geïnstalleerd
- configuraties
- mods en plugins

- scripts
- bestanden
- gebruikers die hij toegang geeft
- activiteiten die via zijn server plaatsvinden

De klant dient redelijke maatregelen te nemen om ongeautoriseerd gebruik van zijn server te voorkomen.

Wanneer een klant een beveiligingsprobleem ontdekt waardoor derden toegang kunnen krijgen tot zijn server, dient hij dit zo snel mogelijk te verhelpen.

3. Wat verstaan wij onder misbruik?

Onder misbruik verstaan wij gebruik van de diensten van PlayNode dat:

- in strijd is met toepasselijke wet- en regelgeving
- andere personen of organisaties schade kan toebrengen
- de infrastructuur van PlayNode of andere klanten kan verstoren
- beveiligingsmaatregelen omzeilt
- de veiligheid van systemen of netwerken in gevaar brengt
- in strijd is met de Algemene Voorwaarden
- of anderszins onredelijk gebruikmaakt van de dienstverlening

Niet ieder hoog resourcegebruik is automatisch misbruik.

Bijvoorbeeld: een zware Minecraft-server, Rust-server of andere game-server kan structureel veel CPU, RAM, opslag of netwerkcapaciteit gebruiken zonder dat dit automatisch een overtreding vormt.

Wanneer gebruik binnen het gekozen pakket en de technische mogelijkheden van de dienst blijft, zal PlayNode dit in beginsel niet als abuse beschouwen.

4. Verboden activiteiten

De volgende activiteiten zijn niet toegestaan via de infrastructuur van PlayNode.

4.1 Illegale activiteiten

Het is niet toegestaan de diensten te gebruiken voor activiteiten die in strijd zijn met toepasselijke wet- en regelgeving.

4.2 Hacking en ongeautoriseerde toegang

Het is niet toegestaan om:

- zonder toestemming toegang te verkrijgen tot systemen van derden
- accounts van derden over te nemen
- beveiligingsmaatregelen te omzeilen
- kwetsbaarheden van derden actief te misbruiken
- ongeautoriseerde toegang tot netwerken of apparaten te verkrijgen

Beveiligingstests zijn uitsluitend toegestaan wanneer de klant daarvoor bevoegd is en de betreffende systemen onder zijn controle vallen of hiervoor expliciete toestemming is gegeven.

4.3 DDoS en andere aanvallen

Het is niet toegestaan de PlayNode-infrastructuur of systemen van derden te gebruiken voor:

- DDoS-aanvallen
- DoS-aanvallen
- reflection- of amplification-aanvallen
- botnetactiviteiten
- andere activiteiten die gericht zijn op het verstoren van de beschikbaarheid van systemen of netwerken

Het is eveneens niet toegestaan om een PlayNode-server bewust te gebruiken als onderdeel van een aanvalsinfrastructuur.

4.4 Malware

Het is niet toegestaan de diensten te gebruiken voor het verspreiden, hosten of beheren van malware, waaronder:

- virussen
- ransomware
- spyware
- trojans
- keyloggers
- botnetsoftware
- andere schadelijke software

Dit geldt niet voor beveiligingsonderzoek of analyse waarbij de klant aantoonbaar bevoegd is en de activiteit geen gevaar vormt voor PlayNode of derden.

4.5 Phishing en fraude

Het is niet toegestaan PlayNode-diensten te gebruiken voor:

- phishing
 - nepwebsites
 - credential harvesting
 - identiteitsfraude
 - betalingsfraude
 - scams
 - misleidende dienstverlening
 - het verzamelen van inloggegevens van derden
-

4.6 Spam

Het is niet toegestaan de infrastructuur te gebruiken voor ongewenste bulkcommunicatie, waaronder:

- spam
- phishingmails
- ongewenste commerciële e-mails

- massale berichten zonder passende toestemming
 - het beheren van spamnetwerken
-

4.7 Scanning en reconnaissance

Het zonder toestemming scannen van systemen, netwerken of apparaten van derden kan als misbruik worden beschouwd.

Dit omvat bijvoorbeeld:

- port scanning
- vulnerability scanning
- brute-force-aanvallen
- geautomatiseerde reconnaissance
- het verzamelen van technische informatie met het doel een systeem aan te vallen

Scans van eigen systemen of systemen waarvoor de klant expliciete toestemming heeft, zijn toegestaan zolang deze geen onredelijke belasting of risico veroorzaken.

5. Illegale of schadelijke content

PlayNode kan optreden tegen inhoud waarvan wij weten of redelijkerwijs moeten aannemen dat deze illegaal is of ernstige schade kan veroorzaken.

Dit kan onder andere betrekking hebben op:

- malware
- phishingmateriaal
- frauduleuze websites
- materiaal dat strafbare activiteiten faciliteert
- content waarvoor PlayNode op grond van een rechtsgeldig bevel verplicht is maatregelen te nemen

PlayNode voert geen algemene voorafgaande controle uit van alle bestanden of inhoud die klanten op hun servers plaatsen.

6. Auteursrecht en intellectueel eigendom

De klant is verantwoordelijk voor het rechtmatig gebruiken van software, games, bestanden, mods, plugins en andere content.

Wanneer PlayNode een voldoende onderbouwde melding ontvangt over mogelijke inbreuk op intellectuele eigendomsrechten, kan PlayNode de melding onderzoeken en passende maatregelen nemen.

Afhankelijk van de omstandigheden kan PlayNode bijvoorbeeld:

- aanvullende informatie opvragen
- de klant verzoeken de betreffende content te verwijderen
- de betreffende dienst tijdelijk beperken
- de dienst opschorten
- verdere maatregelen nemen wanneer dit noodzakelijk of wettelijk vereist is

7. Abuse-meldingen van derden

Iedereen kan een mogelijke abuse-situatie melden bij PlayNode.

Een abuse-melding bevat bij voorkeur:

- naam van de melder
- contactgegevens
- IP-adres of domeinnaam waarop het probleem betrekking heeft
- datum en tijd van het incident
- een duidelijke omschrijving van het vermeende misbruik
- relevante technische informatie
- eventuele bewijsstukken

Meldingen kunnen worden ingediend via:

E-mail: [info@playnode.nl]

PlayNode kan aanvullende informatie opvragen wanneer dit noodzakelijk is om een melding te beoordelen.

8. Beoordeling van abuse-meldingen

PlayNode beoordeelt abuse-meldingen op basis van de beschikbare informatie.

Een melding leidt niet automatisch tot opschorting of beëindiging van een dienst.

Bij de beoordeling kan PlayNode onder andere rekening houden met:

- de ernst van het vermeende misbruik
- de betrouwbaarheid van de melding
- beschikbare technische gegevens
- de mogelijke impact op derden
- de mogelijke impact op PlayNode
- de reactie van de klant
- de vraag of het probleem eenvoudig kan worden opgelost

PlayNode kan technische gegevens en logs gebruiken die rechtmatig beschikbaar zijn om een incident te onderzoeken.

9. Spoedeisende situaties

Wanneer een incident een onmiddellijk en ernstig risico vormt voor:

- de veiligheid van de infrastructuur
- andere klanten
- derden
- persoonsgegevens
- de beschikbaarheid van diensten
- of de continuïteit van PlayNode

kan PlayNode onmiddellijk technische maatregelen nemen.

Dit kan bijvoorbeeld betekenen dat een server tijdelijk:

- wordt geblokkeerd
- netwerktoegang verliest
- wordt geïsoleerd

- wordt opgeschort

Wanneer redelijkerwijs mogelijk wordt de klant hierover zo snel mogelijk geïnformeerd.

10. Maatregelen bij misbruik

Afhankelijk van de ernst en omstandigheden kan PlayNode verschillende maatregelen nemen.

Deze kunnen bestaan uit:

1. Waarschuwing

De klant wordt geïnformeerd over het geconstateerde probleem en krijgt, indien redelijk, de mogelijkheid om dit op te lossen.

2. Verzoek tot aanpassing

PlayNode kan de klant verzoeken bepaalde software, bestanden, configuraties of activiteiten aan te passen of te verwijderen.

3. Tijdelijke beperking

PlayNode kan bepaalde netwerk-, server- of accountfunctionaliteiten tijdelijk beperken.

4. Opschorting

De betreffende dienst kan tijdelijk worden opgeschort.

5. Beëindiging

Bij ernstige of herhaalde overtredingen kan PlayNode de overeenkomst beëindigen overeenkomstig de Algemene Voorwaarden en toepasselijke wetgeving.

6. Wettelijke melding

Wanneer PlayNode daartoe wettelijk verplicht is, kan informatie worden verstrekt aan bevoegde instanties.

11. Geen vaste volgorde bij ernstige incidenten

De bovenstaande maatregelen vormen geen verplichte escalatieladder.

Bij een ernstig incident kan PlayNode direct een passende maatregel nemen zonder eerst een waarschuwing te geven.

Bij minder ernstige situaties probeert PlayNode, waar redelijkerwijs mogelijk, eerst met de klant tot een oplossing te komen.

12. Misbruik door derden via een klantserver

Het kan voorkomen dat een server van een klant wordt misbruikt door een derde, bijvoorbeeld nadat een kwetsbaarheid is uitgebuit.

Wanneer de klant aannemelijk maakt dat hij niet zelf verantwoordelijk is voor het misbruik, zal PlayNode waar redelijkerwijs mogelijk samenwerken aan het beperken en oplossen van het probleem.

De klant blijft verantwoordelijk voor het beveiligen en onderhouden van zijn eigen serveromgeving, tenzij PlayNode hiervoor uitdrukkelijk verantwoordelijk is.

PlayNode kan een server tijdelijk isoleren wanneer dit noodzakelijk is om verdere schade te voorkomen.

13. Compromittering van servers

Wanneer PlayNode aanwijzingen heeft dat een server is gecompromitteerd, kan PlayNode technische maatregelen nemen om verdere schade te voorkomen.

Bijvoorbeeld:

- netwerkisolatie
- tijdelijke opschorting
- reset van bepaalde toegangsgegevens
- blokkeren van bepaalde netwerkverbindingen

Waar redelijkerwijs mogelijk wordt de klant geïnformeerd over de genomen maatregel en de reden daarvoor.

14. DDoS-bescherming

PlayNode kan technische maatregelen inzetten om haar infrastructuur tegen DDoS-aanvallen en andere netwerkdreigingen te beschermen.

DDoS-bescherming betekent niet dat iedere aanval volledig kan worden voorkomen of dat iedere aanval zonder enige impact kan worden opgevangen.

De beschikbare bescherming kan afhankelijk zijn van het gekozen product, de omvang en aard van de aanval en de gebruikte infrastructuur.

15. False positives en onjuiste meldingen

Een abuse-melding kan onjuist, onvolledig of misleidend zijn.

PlayNode probeert daarom relevante meldingen te beoordelen voordat ingrijpende maatregelen worden genomen, tenzij onmiddellijk ingrijpen noodzakelijk is.

Het bewust indienen van valse abuse-meldingen met als doel een andere klant te schaden, kan zelf als misbruik worden beschouwd.

16. Bezwaar tegen een maatregel

Wanneer PlayNode een dienst opschort of andere maatregelen neemt, kan de klant contact opnemen met PlayNode om de situatie toe te lichten.

De klant kan daarbij relevante informatie en bewijs aanleveren.

PlayNode kan een genomen maatregel heroverwegen wanneer nieuwe informatie daar aanleiding toe geeft.

Wettelijke rechten van de klant blijven onverminderd van toepassing.

17. Gegevens en privacy bij abuse-onderzoek

Bij het onderzoeken van abuse kan PlayNode technische gegevens verwerken die noodzakelijk zijn om het incident te onderzoeken.

Dit kan bijvoorbeeld betrekking hebben op:

- IP-adressen
- serverlogs
- tijdstippen
- accountgegevens
- netwerkgegevens
- beveiligingsinformatie

PlayNode verwerkt dergelijke gegevens overeenkomstig haar Privacybeleid en de toepasselijke privacywetgeving.

18. Bewaren van abusegegevens

Gegevens met betrekking tot abuse-incidenten kunnen worden bewaard zolang dit noodzakelijk is voor:

- onderzoek
- beveiliging
- fraudepreventie
- juridische procedures
- het afhandelen van geschillen
- wettelijke verplichtingen

Wanneer de gegevens niet langer noodzakelijk zijn, worden deze verwijderd of geanonimiseerd voor zover dit wettelijk en technisch mogelijk is.

19. Samenwerking met derden

Wanneer dit noodzakelijk is om een ernstig beveiligingsincident of abuse-situatie op te lossen, kan PlayNode samenwerken met:

- datacenterproviders
- netwerkproviders
- beveiligingspartners
- andere infrastructuurleveranciers
- bevoegde instanties

Persoonsgegevens worden daarbij uitsluitend gedeeld wanneer hiervoor een geldige wettelijke grondslag bestaat en voor zover dit noodzakelijk is.

20. Wijzigingen

PlayNode kan dit Abuse & Misbruikbeleid wijzigen wanneer:

- nieuwe vormen van misbruik ontstaan
- de technische infrastructuur verandert
- nieuwe diensten worden toegevoegd
- wet- en regelgeving verandert
- beveiligingsmaatregelen worden aangepast

De meest recente versie wordt op de PlayNode-website gepubliceerd.

De datum bovenaan dit document geeft aan wanneer het beleid voor het laatst is bijgewerkt.

21. Contact

Voor abuse-melding(en), algemene vragen en klantenservice:

[\[info@playnode.nl\]](mailto:info@playnode.nl)

Website:

playnode.nl

Bij een abuse-melding verzoeken wij melders om voldoende technische informatie te verstrekken zodat PlayNode de melding zo effectief mogelijk kan beoordelen.

PlayNode

Dit Abuse & Misbruikbeleid is voor het laatst bijgewerkt op **16 september 2026**.