



Acceptable Usage Policy / Abuse Policy

Index

Index	2
Inleiding	3
Netiquette	4
Abuse Policy.....	5
1. Algemeen.....	5
2. Contact.....	5
3. Wijzigingen	5
Acceptable Usage Policy	6
1. Logingegevens.....	6
2. E-Mail.....	6
3. Netwerk	7
4. Eigen server(s).....	8
5. Usenet.....	8
6. WWW.....	9

Inleiding

Door de toename van breedband internet zijn ook de verschillende vormen van internetmisbruik sterk toegenomen. Hierbij kunt u denken aan bijvoorbeeld spam en virussen, maar ook pogingen tot inbraak op uw computer/netwerk behoren tot wat in zijn algemeen (Internet) Abuse genoemd wordt. Juist om die reden heeft BBeyond een scherp abuse beleid opgezet waarmee we de schade aan ons en uw eigen netwerk minimaliseren om zo te zorgen dat u als klant hier zo weinig mogelijk hinder aan ondervindt.

De voornaamste reden van deze toename is echter dat er steeds meer mensen online zijn zonder dat men de beveiliging van hun computer op orde heeft waardoor de deur als het ware wagenwijd open staat voor alles en iedereen op het internet. Hierdoor loopt men uiteraard het risico om besmet te raken met kwaadwillende virussen die op hun beurt anderen overlast en schade kunnen berokken doordat deze zich graag proberen te verspreiden en vaak een mail-engine ingebouwd hebben waarmee honderden, zo niet duizenden, ongewenste e-mails (spam) verstuurd kunnen worden zonder dat de gebruiker dit merkt.

U als klant en BBeyond als provider zijn dan ook samen verantwoordelijk voor het schoon houden van de eigen netwerken om zo te voorkomen dat andere providers besluiten het verkeer uit het netwerk van BBeyond te weren wanneer er teveel abuse verkeer vandaan komt. Dit kan uiteraard zeer ongewenste gevolgen hebben zoals bijvoorbeeld het niet langer kunnen mailen naar uw zakenpartner op het netwerk van een willekeurige andere provider.

Mocht het voorkomen dat BBeyond constateert dat uw computer/netwerk overlast veroorzaakt dan kan uw verbinding tijdelijk geblokkeerd worden totdat u voldoende maatregelen genomen heeft om deze overlast te stoppen. Op de website <http://www.bbeyond.nl/aup> kunt u lezen welke voorzorgsmaatregelen u kunt nemen en wat de gevolgen zijn van het schenden van onze abuse policy.

Netiquette

Hieronder vindt u de netiquette zoals deze als RFC is opgesteld in 1995 (<ftp://ftp.ripe.net/rfc/rfc1855.txt>). Deze worden algemeen beschouwd als de na te leven omgangsregels op het Internet.

- Er is niets tegen communiceren onder pseudoniem, maar het is niet toegestaan je voor te doen als iemand anders, door bijvoorbeeld afzenderadressen of IP-adressen te vervalsen.
- E-mail zonder encryptie is in principe onveilig en door iedereen te onderscheppen. Zet dus niets in een e-mail dat u niet op een briefkaart zou zetten.
- Wees bewust dat alles wat u op een forum zet, bewaard kan blijven en gelezen zou kunnen worden door bijvoorbeeld een toekomstige werkgever.
- Stuur geen kettingbrieven en spam. Wanneer u kettingbrieven of spam ontvangt, kunt u de netwerkbeheerder van de afzender op de hoogte stellen.
- Het versturen van berichten kost geld voor de verzender, maar ook voor de ontvanger en de eigenaar van het netwerk. Dit is een belangrijke reden waarom spam niet is toegestaan. Om dezelfde reden is het een goed idee e-mailberichten niet te groot te maken. Een bericht met tien foto's als attachment kan een probleem vormen voor de ontvanger en kan het netwerk verstoppen.
- Respecteer de wet op het auteursrecht wanneer u materiaal wilt verspreiden dat u niet zelf gemaakt hebt. Vrijwel alle landen in de wereld hebben zulke wetten. Ook in Nederland mag geen materiaal verspreid worden zonder toestemming van de houder van de auteursrechten.
- Verander geen teksten wanneer u iemand citeert.
- Omdat in communicatie via internet lichaamstaal, gezichtsuitdrukking en intonatie ontbreken, is het extra belangrijk beleefd tegen elkaar te zijn. Iets wat als grapje bedoeld is, kan verkeerd worden opgevat omdat bijvoorbeeld de knipoog ontbreekt.
- Berichten in alleen hoofdletters of met veel uitroeptekens worden algemeen beschouwd als geschreeuw en zijn niet netjes.

Abuse Policy

Middels dit document wil BBeyond haar klanten er op wijzen wat de gevolgen kunnen zijn van het schenden van de Acceptable Usage Policy (AUP).

1. Algemeen

1. Wanneer bij BBeyond klachten ontstaan c.q. van derden worden ontvangen over gedragingen, in strijd met de Acceptable Use Policy, verleent BBeyond zoveel mogelijk medewerking aan de klagende partij om de klacht zo goed mogelijk te onderzoeken. Daarbij worden geen privacy-gevoelige gegevens verstrekt. Wanneer een klacht terecht blijkt te zijn kan BBeyond besluiten de dienst aan de veroorzaker op te schorten, tot er overleg heeft plaatsgevonden tussen de betrokken gebruiker en een bevoegde medewerker van BBeyond. Indien dit overleg niet tot een voor BBeyond bevredigende oplossing leidt, kan zij besluiten de dienst aan de gebruiker met onmiddellijke ingang te staken en de met de gebruiker gesloten overeenkomst met onmiddellijke ingang te ontbinden zoals dit staat vermeld in de Algemene Voorwaarden.
2. Wanneer een gebruiker zich schuldig heeft gemaakt aan opzettelijk spammen zal de dienst waarvoor in deze spamming reclame is gemaakt voor een periode van maximaal 24 uur worden opgeschort. Bij een zeer ernstige overtreding, zulks uitsluitend ter beoordeling van BBeyond, kan deze periode telkens met 24 uur worden verlengd. De opschorting zal duren totdat in overleg met de bewuste gebruiker een voor BBeyond bevredigende oplossing is bereikt om herhaling te voorkomen. Wordt een dergelijke oplossing niet bereikt, dan behoudt BBeyond zich het recht voor de dienst geheel te staken en de overeenkomst met de gebruiker met onmiddellijke ingang buiten rechte te ontbinden.
3. In het geval een gebruiker van de systemen en internetinfrastructuur van BBeyond zich schuldig maakt aan actieve portscans, heeft BBeyond het recht haar dienstverlening aan deze gebruiker met onmiddellijke ingang op te schorten, totdat overleg met de bewuste gebruiker tot een voor BBeyond bevredigende oplossing heeft geleid om herhaling te voorkomen. Wordt een dergelijke oplossing niet bereikt, dan behoudt BBeyond zich het recht voor de dienst geheel te staken en de overeenkomst met de gebruiker met onmiddellijke ingang buiten rechte te ontbinden zoals dit staat vermeld in de Algemene Voorwaarden.

2. Contact

1. Klachten betreffende klanten van BBeyond dienen, vergezeld van internet headers en/of logs in platte text, gericht te worden aan: abuse@bbeyond.nl. Deze afdeling houdt zich bezig met alle vormen van internet abuse en zal uw mail ten alle tijden behandelen maar hierover helaas niet altijd persoonlijk kunnen communiceren.
2. Klanten, welke wegens schending van deze Abuse Policy een opschorting van de dienst ondervinden, dienen contact op te nemen met de Helpdesk van BBeyond welke te bereiken is op 0900-BBEYOND. Bij het herhaaldelijk opschorten van de dienst behoudt BBeyond zich het recht voor heraansluitkosten in rekening te brengen volgens de standaard tarieven; tevens zal wederaansluiting eerst dan plaatsvinden na schriftelijk verzoek van de klant.
3. De Helpdesk van BBeyond zal ten alle tijden de klant informeren wanneer de dienst opgeschort is/wordt.

3. Wijzigingen

1. BBeyond behoudt zich het recht voor aan de hand van maatschappelijke en technische ontwikkelingen deze Abuse Policy eenzijdig te wijzigen.

Acceptable Usage Policy

Dit document beschrijft de voorwaarden die gesteld worden aan het gebruik van de door BBeyond geleverde internetdiensten. Deze Acceptabele Use Policy is van toepassing op het gebruik van het BBeyond netwerk en de diensten die worden verleend door BBeyond. BBeyond behoudt zich het recht voor deze Policy te allen tijde te wijzigen, waarbij het gewijzigde beleid ingaat op het moment dat dit op de volgende locatie is gepubliceerd: <http://www.bbeyond.nl/aup>

- I. Klanten van BBeyond, van partners van BBeyond of van resellers van BBeyond waarvan wordt vastgesteld dat zij deze voorwaarden overtreden (uitsluitend en alleen ter beoordeling van de abuse afdeling van BBeyond) worden onderworpen aan onmiddellijke schorsing en uiteindelijke opheffing van het account zonder restitutie van vooruitbetaalde diensten.
- II. BBeyond kan de klant aansprakelijk stellen voor veroorzaakte schade en voor de kosten die gemaakt worden om deze voorwaarden te handhaven.
- III. Enige daad die resulteert in het onderbreken van de diensten aan andere BBeyond klanten of aan andere internetgebruikers onderwerpt de klant aan onmiddellijke opheffing van het account zonder restitutie van vooruitbetaalde diensten, en kan de klant onderwerpen aan aansprakelijkheid voor de kosten van verloren diensten, plus de kosten van het onderzoek. Dit laat onverlet het recht van BBeyond tot vorderen van schade.
- IV. Enige poging zich ongeoorloofd toegang te verschaffen tot enig systeem, hetzij in het netwerk van BBeyond, hetzij in enig ander netwerk, zal de klant onderwerpen aan disciplinaire maatregelen, tot en met, maar niet beperkt tot, onmiddellijke opheffing van de account zonder restitutie voor vooruitbetaalde diensten, en kan de klant onderwerpen aan aansprakelijkheid voor schade veroorzaakt door het verkrijgen van ongeoorloofde toegang of een poging ongeoorloofde toegang te verkrijgen. Dit laat onverlet het recht van BBeyond tot vorderen van schade.
- V. De klant verklaart zich accoord met het vergoeden van de kosten die BBeyond maakt om enig incident dat in deze Voorwaarden wordt genoemd te onderzoeken en af te wikkelen.
- VI. Klanten zijn verplicht om klachten en problemen betreffende de door klant afgenomen diensten of onder het beheer van de klant vallende apparatuur zo snel mogelijk, maar zeker binnen 24 uur, te melden aan de abuse afdeling van BBeyond. Deze afdeling is enkel en alleen te bereiken via het e-mail adres: abuse@bbeyond.nl

1. Logingegevens

- A. De klant zal identificatiegegevens (login-namen, wachtwoorden), adresgegevens en/of codes met de uiterste zorgvuldigheid bewaren.
- B. Identificatiegegevens, adresgegevens en/of codes mogen niet worden gedeeld met enige andere partij zonder de uitdrukkelijke en schriftelijke toestemming vooraf van BBeyond.
- C. De klant is verantwoordelijk en aansprakelijk voor enig misbruik dat wordt begaan met gebruikmaking van de identificatiegegevens die aan de klant toebehoren, ongeacht de identiteit van de persoon die het misbruik feitelijk pleegt.

2. E-Mail

Het is klanten niet toegestaan om:

- A. ongevraagde commerciële e-mail ('UCE') of ongevraagde bulk e-mail ('UBE') te verzenden naar enige internetgebruiker via een BBeyond-account of via enige andere netwerkverbinding die op enigerlei wijze BBeyond impliceert.
- B. ongevraagde commerciële e-mail ('UCE') of ongevraagde bulk e-mail ('UBE') te verzenden waarin reclame wordt gemaakt voor een bij BBeyond ondergebrachte website, server of andere dienst.
- C. e-mail, al dan niet anoniem, te gebruiken om bedreigende of overlastgevende boodschappen te verzenden.
- D. e-mail te verzenden naar meer dan in totaal 100 adressen zonder voorafgaande toestemming van BBeyond.
- E. enig deel van de header-informatie in een e-mailbericht te vervalsen.
- F. tijdelijk of permanent een onvoldoende beveiligde mailserver aan het netwerk van BBeyond te koppelen. Uw mailserver mag alleen binnenkomende e-mail accepteren die bestemd is voor uw eigen domein(en), en alleen uitgaande e-mail verzenden als die afkomstig is uit uw eigen netwerk/IP-reeks. Uw server mag onder geen beding mail afkomstig van buiten uw netwerk accepteren en deze vervolgens eveneens buiten uw netwerk afleveren. Kortom: uw mailserver moet begin- of eindstation voor e-mail zijn, geen tussenstation. BBeyond behoudt zich expliciet het recht voor een onvoldoende beveiligde mailserver zonder kennisgeving vooraf te blokkeren.

3. Netwerk

Het is klanten niet toegestaan om systemen en/of het netwerk van BBeyond te gebruiken om:

- A. systemen in het netwerk te verstoren.
- B. netwerkdiensten of netwerkcommunicatie te verstoren.
- C. te pogen veiligheidsmaatregelen van enig aan Internet gekoppeld systeem te doorbreken.
- D. de apparatuur, hardware, software, data of diensten van BBeyond te beschadigen of in het ongerede te brengen.
- E. het systeem te gebruiken voor illegale doeleinden.
- F. bedrieglijke on-line marketingpraktijken uit te voeren.
- G. inbreuk te maken op de privacy van individuele gebruikers door middel van het bekijken van hun e-mail of hun private communicatie met andere gebruikers.
- H. bewust of onbewust virussen of andersoortige vormen van malicieuze programma's in het netwerk of systeem te introduceren. De verantwoordelijkheid voor beveiliging tegen virussen of andersoortige vormen van malicieuze programma's ligt bij de klant.
- I. het systeem aan te wenden om zonder toestemming toegang te verkrijgen tot andere computersystemen, netwerken of programma's.
- J. ongeoorloofde toegang te verkrijgen (of pogen te verkrijgen) tot systemen of netwerken, daaronder begrepen enige poging een systeem of een netwerk te proben, scannen of testen op kwetsbaarheden, of om beveiligings- of authenticatiemaatregelen te doorbreken zonder expliciete toestemming van de eigenaar van het systeem of het netwerk.
- K. data of verkeer van enig netwerk of systeem te monitoren zonder expliciete toestemming van de eigenaar van het systeem of het netwerk.
- L. diensten aan een gebruiker, systeem of netwerk te verstoren, inclusief, maar niet beperkt tot, mailbombing, flooding, moedwillige pogingen een systeem te overbelasten, en broadcast-aanvallen.
- M. doelbewust op zoek te gaan naar informatie over anderen, of bestanden, andere gegevens of wachtwoorden van anderen te kopiëren of te wijzigen, of zich voor te doen als een andere gebruiker, tenzij met uitdrukkelijke toestemming van die gebruiker.
- N. inbreuk te maken op wettelijke bescherming van auteursrecht of licentiering van programma's en gegevens.
- O. inbreuk te maken op de integriteit van computer- en netwerksystemen; voorbeeld: klanten zullen niet opzettelijk programma's ontwikkelen of gebruiken die andere gebruikers hinderen of een computer, computersysteem of netwerk infiltreren en/of beschadigen of de software-componenten van een computer, computersysteem of netwerk wijzigen.

- P. enig materiaal te versturen (via e-mail, uploaden, posten of anderszins) dat, opzettelijk of niet, enige toepasselijke nationale of internationale wet, of enige regels die daaruit voortvloeien, overtreedt.
- Q. enig materiaal te versturen (via e-mail, uploaden, posten of anderszins) dat bedreigingen bevat of oproept tot lichamelijk geweld of het vernielen van eigendommen.
- R. enig materiaal te versturen (via e-mail, uploaden, posten of anderszins) dat bij een andere internetgebruiker overlast veroorzaakt.
- S. frauduleuze aanbiedingen te doen om producten, onderwerpen of diensten te kopen of te verkopen, of om enige vorm van financieel bedrog te promoten, zoals (maar niet beperkt tot) "piramide-systemen", "snel rijk worden-systemen" of "kettingbrieven".
- T. identificerende netwerk-header-informatie toe te voegen, te verwijderen of te veranderen met het doel te bedriegen en te misleiden.
- U. te pogen zich als een ander voor te doen door gebruikmaking van vervalste headers of andere identificerende informatie.
- V. toegang te verkrijgen, of pogen toegang te verkrijgen tot de accounts van anderen, of om binnen te dringen, of pogen binnen te dringen, in beveiligingsmaatregelen van de computersoftware of -hardware, elektronische communicatiesystemen of telecommunicatiesystemen van BBeyond of een andere partij, ongeacht of de toegang resulteert in beschadiging of verlies van gegevens.
- W. enig materiaal te versturen (via e-mail, uploaden, posten of anderszins) dat inbreuk maakt op auteursrecht, handelsmerk, patent, handelsgeheim of andere eigendomsrechten van een derde partij, inclusief, maar niet beperkt tot, het ongeoorloofd kopiëren van auteursrechtelijk beschermd materiaal, het digitaliseren en distribueren van fotomateriaal uit tijdschriften, boeken of andere auteursrechtelijk beschermde bronnen, en het ongeoorloofd verzenden van auteursrechtelijk beschermde software.
- X. persoonlijke gegevens van derden te verzamelen, of pogen te verzamelen, zonder hun medeweten of instemming.

4. Eigen server(s)

Alle apparatuur die via een door BBeyond geleverde verbinding op het Internet aangesloten wordt dient voldoende beveiligd te zijn. BBeyond behoudt zich expliciet het recht voor onvoldoende beveiligde apparatuur zonder kennisgeving vooraf te blokkeren of af te sluiten.

Onder een goede beveiliging vallen onder meer, maar niet uitsluitend:

- A. een mailserver mag niet als tussenstation gebruikt kunnen worden zoals omschreven in punt 2F van dit document.
- B. een webserver mag niet als tussenstation of proxyserver gebruikt kunnen worden door derde partijen.
- C. Een SOCKS-compatible server mag niet gebruikt kunnen worden door derde partijen. SOCKS documentatie is te vinden op <http://www.socks.nec.com>.
- D. Overige apparatuur en diensten moeten op een zodanige manier beveiligd zijn dat het niet mogelijk is voor derde partijen om de apparatuur of dienst te gebruiken als tussenstation voor enige vorm van communicatie over het Internet.
- E. De apparatuur moet beveiligd zijn tegen computer-virussen en andere vormen van zichzelf verspreidende en/of schadelijke software.
- F. De apparatuur moet beveiligd zijn tegen ongeoorloofde toegang door derden.

De klant blijft verantwoordelijk voor *alle* activiteiten die worden uitgevoerd door middel van de apparatuur die door de klant wordt beheerd. Ook indien deze activiteiten door een derde partij zijn veroorzaakt zonder dat de klant daarvan op de hoogte was.

5. Usenet

Het is klanten niet toegestaan om:

- A. berichten naar een nieuwsgroep te posten die niet voldoen aan het gepubliceerde charter van die nieuwsgroep.
- B. berichten die opruiend van aard zijn en bedoeld zijn om conflicten uit te lokken tussen gebruikers van die nieuwsgroepen te kruisposten naar meerdere nieuwsgroepen.
- C. berichten te posten die op ongepaste wijze een product, website of dienst adverteren, hetzij door dit herhaald te doen of door het bericht te kruisposten naar verschillende nieuwsgroepen die anderszins niet met elkaar in verband staan (ook wel bekend als 'Spam').
- D. commerciële postings te doen naar niet-commerciële nieuwsgroepen.
- E. postings te doen die zijn gericht aan ontoepasselijke of niet-gerelateerde groepen, of te posten naar meer dan 15 groepen tegelijkertijd.
- F. identieke berichten meerdere malen te posten, ongeacht het aantal nieuwsgroepen.
- G. enig deel van de header-informatie van een nieuwsgroep-posting te vervalsen, met als enige uitzondering het vervormen van het afzendadres om spam te voorkomen ("munging").

6. WWW

BBeyond behoudt zich het recht voor enige door de klant geproduceerde informatie, die als aanstootgevend wordt beoordeeld door leden van de Internetgemeenschap, de directie van BBeyond, of onwettig is volgens nationale of internationale wetgeving (specifiek, maar niet uitsluitend, beschermd materiaal), van zijn servers te verwijderen. Onder 'aanstootgevend' wordt tevens verstaan het adverteren van de website op een wijze die in artikel 2 en 5 van deze AUP wordt verboden ('spamvertizing'), waarbij het niet van belang is of het adverteren van de website via een andere ISP plaatsvindt. Herhaalde klachten kunnen resulteren in het opheffen van het account van de klant en het verwijderen van opgeslagen gegevens zonder voorafgaande kennisgeving.