

Acceptable use policy

Nieuwste publicatie op 1 december 2016

Door middel van dit document wil de Webbouwmeester ('Leverancier') de gebruikers van haar systemen en haar internetinfrastructuur wijzen op de gevolgen van schending van de "Acceptable Use Policy".

ALGEMEEN

In het geval een gebruiker van de systemen en internetinfrastructuur van Leverancier zich schuldig maakt aan actieve portscans, heeft Leverancier het recht haar dienstverlening aan deze gebruiker met onmiddellijke ingang op te schorten, totdat overleg met de bewuste gebruiker tot een voor Leverancier bevredigende oplossing heeft geleid om herhaling te voorkomen. Wordt een dergelijke oplossing niet bereikt, dan behoudt Leverancier zich het recht voor de dienst geheel te staken en de overeenkomst met de gebruiker met onmiddellijke ingang te ontbinden.

Klachten

Copyright en Merkenrecht

Indien er klachten zijn wegens schending van derdenrechten jegens een klant, beslist de klant in eerste instantie zelf wat er met haar account gebeurt. Hier wordt alleen af van geweken indien rechtenschending van derden blijkt uit schriftelijke en uitgebreide bewijsvoering door de partij wiens rechten zijn geschonden, en nadat Leverancier na haar eigen interpretatie van mening is dat belemmering van deze schending dringend van aard is. In alle andere gevallen wordt er door de Webbouwmeester geen actie ondernomen tot het moment waarop belemmering gerechtelijk onderschreven wordt.

Spam klachten

Voor de klachten behandeling betreffende spam, verwijzen we u naar ons SPAM-beleid.

Klachten ten gevolge van account misbruik / onervaren gebruik

Deze klachten kunnen voort komen uit netwerkproblemen en/of performance problemen met de server waar de producten die u afneemt aan gelinkt zijn. Hiervoor verwijzen we u naar het Hacking/portscans beleid en Scripting beleid.

Wijziging

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

Acceptable Use Policy

Door middel van dit document wil Leverancier haar klanten en gebruikers wijzen op hun verantwoordelijkheden wanneer zij van de internetfaciliteiten van Leverancier gebruik maken. Wanneer bepalingen uit deze Acceptable Use Policy worden overtreden, kan Leverancier die

maatregelen treffen, omschreven in deze Acceptable Use Policy om overtreding daarvan voortdurend te voorkomen.

Doel van deze Acceptable Use Policy is onder meer:

- de gebruikers van de internetfaciliteiten van Leverancier en daaraan verbonden netwerken veilig en betrouwbaar Internetverkeer te bieden;
- situaties te vermijden die kunnen leiden tot aansprakelijkheid;
- bijdragen aan een positieve beeldvorming en goede reputatie van Leverancier als een verantwoordelijke internetprovider;
- bijdragen aan de waarde van internetresources als een platform voor vrije meningsuiting;
- het bevorderen van het verantwoordelijk gebruik van het internet en het ontmoedigen van praktijken die de bruikbaarheid en daarmee de waarde van het internet negatief beïnvloeden;
- het beschermen van de privacy en (internet-)veiligheid van de individuele gebruikers van de diensten van Leverancier.

Algemene gedragsregels:

- Uitgangspunt is dat gebruikers van het netwerk en de internetinfrastructuur van Leverancier zich als goed en zorgvuldig internetgebruikers zullen gedragen en geen overlast zullen veroorzaken voor andere gebruikers en/of netwerken op het internet.
- De gebruiker van de diensten van Leverancier is gehouden de redelijke instructies van Leverancier ten aanzien van de geboden internetdiensten op te volgen.
- Gebruikers zullen zich onthouden van het doen verzenden via of plaatsen op het internet van enig materiaal, in welke uitdrukkingvorm ook, dat kan worden beschouwd als onwettig, obscene, bedreigend, discriminerend, smadelijk danwel materiaal of uitingen die gedragingen aanmoedigen of uitlokken dat kunnen worden beschouwd als strafbaar feit of welk gedrag aanleiding kan geven voor civielrechtelijke aansprakelijkheid of op enige andere wijze in strijd is met de Nederlandse wet of internationale regelgeving.
- Wanneer bij Leverancier klachten ontstaan c.q. van derden worden ontvangen over gedragingen, in strijd met de Acceptable Use / Abuse Policy, verleent Leverancier 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 de Webbouwmeester besluiten de dienst aan de veroorzaker op te schorten, tot er overleg heeft plaatsgevonden tussen de betrokken gebruiker en een bevoegde medewerker van Leverancier. Indien dit overleg niet tot een voor Leverancier 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.
- Ter bevordering van een goed en zorgvuldig internetgebruik zal het de gebruiker van de systemen en internetinfrastructuur van Leverancier uitdrukkelijk verboden zijn virussen of andersoortige vormen van kwaadwillige programma's in het netwerk of internetinfrastructuur te introduceren. De gebruiker zal alles doen wat redelijkerwijs mogelijk is om te voorkomen dat een computervirus of ander kwaadwillig programma op het internet of in de netwerken of internetinfrastructuur van Leverancier kan komen.
- De gebruiker van de systemen en internetinfrastructuur van Leverancier zal een zodanig gebruik maken van de diensten van Leverancier dat daardoor de juiste werking van het netwerk en de internetinfrastructuur van Leverancier niet wordt belemmerd of gehinderd, danwel dat daardoor andere gebruikers van de systemen en internetinfrastructuur van Leverancier worden belemmerd of gehinderd.

Accounts en wachtwoorden:

- De gebruiker van de systemen en internetinfrastructuur van Leverancier zal de hem toegekende identificatiegegevens als wachtwoorden, loginnamen, user-id's etc. met de uiterste zorgvuldigheid bewaren en nimmer aan derden kenbaar maken. Dergelijke gegevens mogen, behoudens voorafgaande schriftelijke toestemming van Leverancier niet worden gedeeld met derden.
- Als uitzondering op lid 1 geldt dat indien de cliënt als reseller optreedt deze wachtwoorden mag uitwisselen met de cliënt waarvoor de opdracht bij de Webbouwmeester plaats vond.
- De gebruiker van de systemen en internetinfrastructuur van Leverancier is uitsluitend verantwoordelijk en aansprakelijk voor ieder misbruik dat wordt gemaakt met behulp van zijn identificatiegegevens, ongeacht de identiteit van de persoon die het misbruik feitelijk pleegt.
- Wachtwoorden en identificatiegegevens worden door Leverancier als geldige handtekening beschouwd voor het bestellen van producten en diensten.

Hacking/portscans beleid:

- De gebruiker van de systemen en infrastructuur van Leverancier zal zich onthouden van iedere poging om, op welke wijze dan ook, ongeautoriseerd geautomatiseerde systemen van derden onbevoegd binnen te dringen, zich toegang te verschaffen tot gegevens die niet voor de gebruiker bestemd zijn, in te loggen op een server of account waartoe de gebruiker niet bevoegd is c.q. geen rechten heeft.
- De gebruiker van de systemen en de internetinfrastructuur van Leverancier zal zich onthouden van alle activiteiten, van welke aard en uitingsvorm ook, die gericht zijn op het testen van de beveiliging van de systemen en/of infrastructuur van Leverancier en/of netwerken, servers en bestanden van derden op het internet.
- De gebruiker van de systemen en internetinfrastructuur van Leverancier zal zich onthouden van alle activiteiten die inbreuk kunnen maken op de diensten van Leverancier (DoS-attacks). Hieronder wordt onder meer begrepen het genereren van een "overstroom/flooding" van dataverkeer, opzettelijke pogingen om een dienst te overbelasten en pogingen om een dienst te laten "crashen".
- Gebruikers van de systemen en internetinfrastructuur van Leverancier zullen zich onthouden van het gebruik van programma's, scripts, commando's of boodschappen van welke inhoud ook, ontworpen om in te breken in het internetverkeer van derden. Dit verbod geldt niet voor statistische metingen op de eigen websites.
- Portscans kunnen schadelijk zijn voor de internetomgeving. Portscans worden in de internetwereld als een agressieve handeling opgevat. Portscans kunnen derhalve afbreuk doen aan de goede reputatie van Leverancier als internetprovider. Gebruikers van de systemen en internetinfrastructuur van Leverancier zullen zich derhalve dienen te onthouden van portscans.
- In het geval een gebruiker van de systemen en internetinfrastructuur van Leverancier zich schuldig maakt aan actieve portscans, heeft Leverancier het recht haar dienstverlening aan deze gebruiker met onmiddellijke ingang op te schorten, totdat overleg met de bewuste gebruiker tot een voor Leverancier bevredigende oplossing heeft geleid om herhaling te voorkomen. Wordt een dergelijke oplossing niet bereikt, dan behoudt Leverancier zich het recht voor de dienst geheel te staken en de overeenkomst met de gebruiker met onmiddellijke ingang te ontbinden.

Scripting beleid:

Spammen / ongewenste email:

Waarom? In tegenstelling tot de traditionele verspreiders van "junk mail", die postpapier, enveloppen en port betalen, kunnen verspreiders van Unsolicited Bulk E-mail (UBE) en Unsolicited Commercial E-mail (UCE), oftewel grote hoeveelheden ongevraagde commerciële e-mail (ook wel spam genoemd), zonder al te veel kosten aan hun eigen zijde voor grote overlast en enorme kosten zorgen aan de zijde van de ontvangers van dergelijke e-mail.

Deze kosten zijn o.a.:

- Bandbreedte van de ISP om spam te verspreiden; Additionele IP infrastructuur
- Het signaleren, filteren en verwijderen van spam (UBE en UCE)
- Uitbreiding van de infrastructuur met hard- en software voor de benodigde voorzorgsmaatregelen

Leverancier is van mening dat de bovenstaande kosten niet zonder meer aan de gebruikers van het Internet kunnen worden opgedrongen. Het uitbannen van spam zal volgens Leverancier leiden tot een beter en goedkoper gebruik van het Internet en stelt Leverancier beter in staat haar klanten een efficiënte en betaalbare service te verlenen.

Indien u voor uw site reclame wilt maken, gebruik dan alstublieft een ander middel. Het probleem is dat bijna niemand positief reageert op spam berichten. Veel mensen gaan boze e-mail sturen, en vaak komt deze e-mail bij de provider (dus ons) terecht. Wij zijn verplicht deze te beantwoorden. Doen wij dit niet, dan wordt Leverancier naar alle waarschijnlijkheid opgenomen in allerlei anti spam filters, waar wij en onze andere klanten dan de dupe van worden.

SPAM-beleid

A. Het is klanten verboden om spam berichten te verzenden aan derden die hierom niet nadrukkelijk hebben verzocht; Hetzij via het netwerk van Leverancier, hetzij ter promotie van een website die via het netwerk van Leverancier met het Internet is verbonden. Hieronder is ook spam begrepen die via elke andere provider wordt verstuurd met referentie aan een website, e-mail adres of andere dienst bij Leverancier en/of berichten in meerdere nieuwsgroepen tegelijk (crosspost) en/of afzonderlijk (multipost) posten met daarin reclame of andere commerciële uitingen voor een domein en/of een emailadres en/of welke andere dienst dan ook, danwel aan individuele emailadressen te versturen. Dit geldt tevens indien deze handelingen worden verricht bij een andere provider maar de bedoelde website wordt gehost bij Leverancier. Tevens is het klanten verboden derden ongevraagd te abonneren op mailinglijsten.

B. Het is klanten verboden om tijdelijk of permanent met een onvoldoende beveiligde mail server verbonden te zijn in het netwerk van Leverancier. De mailserver is toegestaan om inkomende e-mail te accepteren dat is bedoeld voor de desbetreffende domein(en), en e-mail te verzenden dat afkomstig is van het door Leverancier toegekende IP adres(sen). Het is expliciet verboden e-mail te accepteren buiten het toegekende netwerk welke bedoeld is voor verzending buiten dit netwerk. Anders gezegd: de mailserver is het begin of het eindpunt voor e-mail, geen tussenstation. Leverancier heeft het recht om een onvoldoende beveiligde mail server zonder kennisgeving vooraf te blokkeren op het Internet.

C. Bulk e-mail is toegestaan indien gebruik wordt gemaakt van de zogenaamde verified OPT-IN regeling. Mailings waar een database voor is gebruikt waarin de ontvanger de verzender (de klant) niet heeft geautoriseerd, worden behandeld als spam en Leverancier zal dit bij de ontvangst van klachten als zodanig behandelen.

D. Klachten betreffende spam dienen te worden ingediend per e-mail op abuse @ firstfind.nl. De klacht moet een volledige kopie inclusief originele headers van de mogelijke spam e-mail bevatten. Nadat is vastgesteld of de klacht daadwerkelijk UBE of bulk UCE betreft, krijgt de klant een officiële waarschuwing: FTO ("First Time Offender"). Indien binnen 24 uur geen reactie volgt waaruit blijkt dat er voldoende maatregelen zijn genomen om spam te voorkomen, behoudt Leverancier zich het recht voor, de door Leverancier toegekende IP adres(sen) of site van het Internet te weren.

E. Gefundeerde klachten over een klant die reeds bekend staat als FTO zullen er toe leiden dat Leverancier zonder kennisgeving vooraf de respectievelijke DNS records steeds voor een periode van minimaal 48 uur zal verwijderen. De klant wordt op de hoogte gesteld dat deze de status van STO ("Second Time Offender") heeft verworven. Leverancier houdt zich het recht voor de dienst aan de klant zonder enig recht op kostenvermindering voor de nog lopende abonnementstermijn, definitief op te heffen. Als een onvoldoende beveiligde server is gebruikt voor het verzenden of doorsturen van spam, wordt poort 25 (SMTP) geblokkeerd voor het (de) respectievelijke IP adres(sen).

F. Klanten die voor de derde maal de fout ingaan (TTO, "Third Time Offenders") worden altijd onherroepelijk afgesloten zonder enig recht op kostenvermindering voor de nog lopende abonnementstermijn.

G. Leverancier heeft het recht om dataverkeer te blokkeren van andere netwerken om zodanig spam te weren of te voorkomen. Het is mogelijk dat dit kan leiden tot tijdelijke uitval van verbinding(en) met andere netwerken.

Email:

Het is gebruikers van de systemen en internetinfrastructuur van Leverancier niet toegestaan om:

- email, al of niet anoniem, te gebruiken om bedreigende of overlastgevende boodschappen te verzenden;
- enig deel van de headerinformatie in een emailbericht te vervalsen;
- tijdelijk of permanent een onvoldoende beveiligde mailserver aan het netwerk van Leverancier te koppelen. De mailserver behoort alleen binnenkomende email te accepteren die bestemd is voor eigen domeinen en alleen uitgaande email verzenden als die afkomstig is uit het eigen netwerk/IP-reeks. De mailserver mag niet als tussenstation worden gebruikt ten behoeve van mail die niet voor de gebruiker zelf of op diens intranet aangesloten gebruikers bestemd is.

Wijziging:

Leverancier behoudt zich het recht voor aan de hand van maatschappelijke en technische ontwikkelingen deze Acceptable Use Policy eenzijdig te wijzigen.