

# Acceptable Use Policy

December 2003



## Inhoud

I. Inleiding.....	3
II. Wettelijke bepalingen.....	3
III. Verbod op activiteiten.....	4
A. Verboden activiteiten: algemeen.....	4
B. Verboden activiteiten: systeem en netwerk beveiliging .....	5
C. Verboden activiteiten: e-mail .....	6
D. Verboden Activiteiten: usenet (nieuwsgroepen).....	7
E. Verboden activiteiten: inbel-accounts .....	8
F. Verboden activiteiten: webruimte .....	9
IV. Klachten en naleving afdwingen .....	10
Klachten.....	10
Naleving afdwingen.....	10
Aansprakelijkheid.....	10
V. Overige bepalingen.....	11

### I. Inleiding

Deze Acceptable Use Policy ('AUP') bevat een aantal regels voor het gebruik van de systemen, diensten en producten door klanten van Netland Internet Services te Amsterdam (verder te noemen 'Netland'). De AUP is ingesteld ter bevordering van de veiligheid, betrouwbaarheid en privacy van de systemen, netwerken en klanten van Netland. Overtreding van de AUP kan in het ergste geval leiden tot onmiddellijke stopzetting van de geleverde diensten en/of producten.

Indien een internetgebruiker zich niet aan de regels houdt, zoals vermeldt in de AUP, kunt u hier melding van maken door een e-mail te sturen naar [abuse@netland.nl](mailto:abuse@netland.nl). Vermeld hierin alle relevante informatie. Meer informatie vindt u in paragraaf F.

### II. Wettelijke bepalingen

Het is niet toegestaan software te versturen, door te sturen of te bewaren op of middels systemen, diensten of producten van Netland waarvoor geldt dat deze:

1. in strijd is met de Nederlandse wetgeving.
2. bedreigend, onzedelijk, onfatsoenlijk of kwetsend is, of ongunstige gevolgen kan hebben voor een individu, groep of instantie.
3. de rechten schendt van een (rechts-)persoon (inclusief rechten beschermd door copyright, trade secret, patent en/of ander intellectueel eigendom of vergelijkbare wetten/regels), inclusief de installatie of distributie van illegale of andere software waarvoor de klant geen geldige licentie heeft.

### III. Verbod op activiteiten

Deze AUP definieert activiteiten die Netland als 'misbruik' bestempelt en die dus verboden zijn. Indien de klant niet zeker weet of een bepaalde activiteit wel of niet in strijd is met deze AUP, dient deze vooraf een e-mail te sturen naar [abuse@netland.nl](mailto:abuse@netland.nl). Netland zal hierover dan een uitspraak doen.

De in de volgende paragrafen genoemde activiteiten zijn niet allesomvattend en zijn deels als indicatie bedoeld.

Het onderstaande gebruik / toepassingen van de systemen, diensten en producten van Netland zijn expliciet verboden (A t/m F) :

#### A. Verboden activiteiten: algemeen

1. Het overbrengen of bewaren van materiaal, informatie of andere data die in de ogen van Netland onwettelijk, onzedelijk, bedreigend of kwetsend kan zijn of kan leiden tot verkeerd gebruik, aanmoedigt tot onwettelijk gedrag of op enige andere wijze strijdig is met de lokale, landelijke of internationale wetgeving, op of met systemen, diensten of producten van Netland is verboden.
2. Het schenden van rechten van (rechts-)personen waaronder het copyright, trade secret, patenten, het intellectueel eigendom of vergelijkbare wetgeving.
3. Activiteiten die moeilijkheden veroorzaken voor klanten, medewerkers van Netland of andere internetgebruikers, in het gebruik van de systemen, diensten en/of producten van Netland.
4. Doorverkoop van systemen, diensten en/of producten van Netland zonder uitdrukkelijke schriftelijke toestemming van Netland.
5. Misleidende online marketing activiteiten.
6. Het verschaffen van valse gegevens in een (online) formulier, contract of enige andere (online) applicaties, inclusief vervalste creditcardnummers. Deze activiteiten kunnen leiden tot onmiddellijke verbreking van bestaande contracten en afspraken en kunnen leiden tot wettelijke aansprakelijkheid van de overtreder.

## B. Verboden activiteiten: systeem en netwerk beveiliging

1. Pogingen tot het ontwijken van de user-identificatie of enige vorm van beveiliging van een host, netwerk of account (aangeduid met de term 'hacking'). Hieronder vallen onder andere het zich toegang verschaffen tot data die niet bestemd is voor de klant, het inloggen op een server of account waarvoor de klant geen expliciete toestemming heeft of (een poging tot) het ondermijnen van de beveiliging van andere netwerken (zoals bijvoorbeeld het runnen van SATAN of een dergelijk programma).
2. Het veroorzaken van een 'beveiligingsbreuk' of 'verstoring' van de internetcommunicatie. Onder beveiligingsbreuken vallen onder andere: het zich toegang verlenen tot data die niet bestemd is voor de klant of het inloggen op een server zonder het expliciete recht tot toegang.  
Onder 'verstoring' worden in deze paragraaf onder andere gerekend: port scans, ping floods, packet spoofing, vervalsing van routing informatie, opzettelijke pogingen tot het overbelasten van een dienst en pogingen tot het laten crashen van een host.
3. Het gebruik of uitvoeren van programma's, scripts, commando's of het versturen van berichten (in welke vorm dan ook) met de bedoeling een gebruiker te hinderen (lokaal of via internet).
4. Het uitvoeren van enige vorm van netwerkobservatie die kan lijden tot het onderscheppen van data die niet bestemd is voor de klant.

## C. Verboden activiteiten: e-mail

1. Het 'treiteren' van ontvangers middels taal, frequentie of grootte van berichten is verboden.
2. Het versturen van ongevraagde e-mail (met inbegrip van 'junk mail' of ander reclame materiaal) naar individuen die hier niet expliciet om gevraagd hebben (ook wel genoemd 'spam'). Hieronder vallen onder andere volume-zendingen van reclame, informatieve documenten en politieke boodschappen. Deze boodschappen mogen alleen verstuurd worden wanneer de ontvanger hier expliciet om gevraagd heeft. Als een ontvanger vraagt om stopzetting van de mail, moet de zender de zending van verdere mail onmiddellijk stoppen. De zender dient hiervoor een mogelijkheid te bieden in het bericht.
3. Het aanmaken of doorsturen van 'kettingbrieven' of 'piramide systemen' van enige soort, ongeacht of de ontvanger hierom gevraagd heeft.
4. Kwaadwillig e-mail. Hieronder valt onder andere het versturen van een 'mailbom' (het overspoelen van een user of site met een grote hoeveelheden e-mail)
5. Onbevoegd gebruik of vervalsing van e-mail header informatie.
6. Het gebruiken van een intern Netland-account of van een account van een klant van Netland, om antwoorden op een mailing te vergaren, verstuurd vanaf een ander provider.
7. Het versturen van ongevraagde e-mail die zijn oorsprong heeft bij het Netland-netwerk of bij netwerken van andere providers, met hierin reclame-uitingen voor diensten gehost door Netland.
8. Het opzettelijk niet of onvoldoende beveiligen van SMTP poorten, met de bedoeling het toelaten van derden op de server voor het versturen van e-mail.

### D. Verboden Activiteiten: usenet (nieuwsgroepen)

1. Het posten van dezelfde of bijna dezelfde boodschappen naar veel verschillende nieuwsgroepen (ook wel 'nieuwsgroep spam' of 'usenet spam').
2. Het versturen van ketting brieven via usenet.
3. Het versturen van (gecodeerde, binaire) files naar nieuwsgroepen die daar niet expliciet voor bedoeld zijn.
4. Het annuleren ('cancellen') van berichten ander dan eigen berichten. Uitzondering hierop vormen de officiële nieuwsgroep moderators voor wie dit tot hun takenpakket hoort.
5. Het vervalsen van header informatie, inclusief pogingen tot het ontwijken van het controleproces ('approval') voor het posten in gesloten nieuwsgroepen.
6. Het versturen van berichten met de bedoeling reacties te verzamelen voor een ander e-mail adres of dienst dan die van de zender.
7. Het versturen naar nieuwsgroepen van boodschappen die strijdig zijn met de regels of FAQ's van de betreffende nieuwsgroep is niet toegestaan. Degene die een bericht verstuurt is verplicht vooraf na te gaan wat wel en niet mag bij een bepaalde nieuwsgroep, bijvoorbeeld door het raadplegen van de FAQ's in nl.internet.welkom.
8. Het posten van usenet artikelen vanaf het Netland-netwerk of het netwerk van een andere provider met de bedoeling tegen de regels van de nieuwsgroep in reclame te genereren voor diensten gehost door Netland of verbonden aan de Netland-netwerk.
9. Het opzettelijk niet of onvoldoende beveiligen van een news server, zodat een derde partij toegang heeft tot de server, wat zouden kunnen leiden tot het versturen van berichten naar een nieuwsgroep.

## E. Verboden activiteiten: inbel-accounts

1. Het dubbel inbellen bij Netland is niet toegestaan, mits er door Netland uitdrukkelijk toestemming is verleend.
2. Gebruikersnamen die lijken op commando's, overkoepelende organen of andere veel gebruikte termen (tia, gov, exit) worden niet toegestaan.
3. Gebruikers van shell accounts (telnet) mogen geen diensten aanbieden (zoals IRC, MUD servers) aan derden vanuit hun accounts.
4. Pogingen tot het omzeilen van de 'idle daemon' of het omzeilen van tijdregistratie of pogingen programma's te draaien zonder in te loggen, zijn verboden.
5. Het delen van passwords of accounts met anderen is niet toegestaan.

## F. Verboden activiteiten: webruimte

1. Het buitensporig gebruik van systeembronnen, inclusief CPU tijd, geheugen, disk ruimte en sessietijd. Het zonder uitdrukkelijke toestemming gebruiken van programma's die intensief gebruik maken van de middelen van Netland of die een negatieve invloed hebben op het functioneren van de systemen van Netland is verboden. In dit geval kan de staf van Netland actie ondernemen en de toegang tot de systeembronnen voor deze programma's beperken of de programma's afsluiten, zonder vooraf overleg met de klant.

## IV. Klachten en naleving afdwingen

### Klachten

Indien u een klacht over wangedrag wilt doorgeven aan Netland, stuurt u een bericht naar: [abuse@netland.nl](mailto:abuse@netland.nl)

Netland Internet Services  
Kruislaan 419  
1098 VA Amsterdam  
fax: 020-5628281

Klachten via e-mail worden alleen in behandeling genomen wanneer er een volledige naam en adres is vermeld. Anonieme klachten worden niet in behandeling genomen. Voordat Netland actie kan ondernemen moet misbruik te bewijzen zijn. Vermeld bij uw melding daarom altijd het tijdstip en indien van toepassing alle e-mail headers. Om te constateren welke weg een boodschap heeft gevolgd en of een boodschap gedeeltelijk of geheel is vervalst, heeft Netland de gehele boodschap nodig. Deze informatie is noodzakelijk voor het onderzoek.

### Naleving afdwingen

Naar eigen inzicht kan Netland te allen tijde en zonder voorafgaande waarschuwing, naar aanleiding van activiteiten die tegenstrijdig zijn tot deze AUP bepaalde diensten van een klant tijdelijk of permanent afsluiten. In het algemeen zal Netland bij een eerste waarschuwing een klant desgewenst voorlichten om te voorkomen dat de klant in herhaling valt. Netland zal slechts in het uiterste geval overgaan tot het tijdelijk of permanent afsluiten van bepaalde diensten.

### Aansprakelijkheid

Op geen enkele mogelijke manier kan Netland aansprakelijk gesteld worden door een klant of een derde partij, voor directe of indirecte schade in welke vorm dan ook, als gevolg van activiteiten die in strijd zijn met de AUP. Netland is niet aansprakelijk voor onder andere winst verlies, werkonderbreking, verlies van software of data, ook al is Netland vooraf geadviseerd over de kans van dergelijk schade.

## V. Overige bepalingen

1. **Wijziging AUP**  
Netland houdt zich het recht voor om de AUP te allen tijde te veranderen. Elke wijziging is met onmiddellijke ingang geldig voor alle klanten. De AUP is ten aller tijde gratis te downloaden van de site van Netland (<http://www.netland.nl>). Wijzigingen zullen bekend worden gemaakt via de gratis nieuwsbrief van Netland, 'NL-Nieuws'. Hiervoor dient u zichzelf op te geven via de eerder genoemde website.
2. **Applicatie van de AUP**  
De bepalingen zoals opgenomen in deze AUP, worden ook nagestreefd door andere providers.
3. **Verantwoordelijk voor content**  
Netland kan op geen enkele manier verantwoordelijk worden gesteld voor de inhoud ('content') van publicaties door klanten, waaronder e-mail, postings in nieuwsgroepen en sites.
4. **Verwijderen van data**  
Naar eigen inzicht kan Netland in het uiterste geval ten alle tijden materiaal of data van haar servers verwijderen of de internettoegang sluiten indien Netland een schending van de AUP door een klant vermeent.
5. **Virussen**  
Alle e-mail van klanten van Netland, met uitzondering van klanten met een eigen mailserver of een @netland.nl e-mailadres, wordt op virussen gescand. De scanner wordt regelmatig ge-update. Indien een virus wordt ontdekt, wordt de betreffende e-mail vernietigd. De zender en de beoogde ontvanger van het bericht ontvangen een waarschuwing per e-mail. Netland doet dit omdat:
  - Klanten grote hinder ondervinden van virussen en gegevens kunnen verliezen en/of ongewild (bedrijfsgevoelige) informatie kunnen verspreiden.
  - Onze mailservers en mailservers van andere providers overbelast kunnen raken waardoor de dienstverlening ernstig in gevaar kan komen.

Nadrukkelijk willen we stellen dat we het onze verantwoordelijkheid vinden, virussen voor klanten zo goed als mogelijk tegen te houden. Een virusscanner is echter nooit 100% waterdicht. Daarnaast kan de scanner bijvoorbeeld niet bestanden die gedownload worden scannen. Netland is niet aansprakelijk voor welke vorm van schade dan ook, (in) direct veroorzaakt door (het niet tegenhouden van) virussen.

### Privacy

De virusscanner kijkt of iedere e-mail een bepaalde reeks karakters bevat dat overeenkomt met een virus. Dit gebeurt geheel automatisch. Nadrukkelijk willen we stellen dat Netland in geen gevallen (persoons-) gegevens zal opslaan, zal gebruiken voor (marketing) acties of zal verhandelen. De data voor de statistieken op de Netland website is zuiver een telling en wordt meteen losgekoppeld van enige persoonsgegevens.