Fair Use Policy SSHnet

1. Definities

- SSH: de eigenaar van het netwerk.
- SSHnet: het computernetwerk op huisvestingcomplexen van en in woningen van de SSH.
- netwerkbeheerder: de door de SSH aangewezen netwerkbeheerder.
- CERT-SSH/Helpdesk SSHnet: een door de SSH aangewezen organisatie die voor de SSH leiding geeft aan het afhandelen van misbruikgevallen op het SSHnet.
- Helpdesk SSHnet/abusegroep: een organisatie op een SSH complex die misbruikgevallen afhandelt.
- gebruiker: de huurder; de persoon die een huurovereenkomst heeft met de SSH voor een ruimte met een netwerkaansluiting.
- Policy: de inhoud van dit document.

2. Algemeen

SSHnet-gebruikers dienen zich te houden aan de volgende wetgeving en regels:

- de Nederlandse wetgeving;
- het Reglement gebruik ICT middelen van de Universiteit Utrecht, met deze toelichting;
- de internet gebruiksvoorwaarden van de SSH;
- de Fair Use Policy van de SSH (dit document);
- de gedragsregels voor het SSHnet zoals neergelegd in deze policy;
- netiquette.

In het geval van conflicten of tegenstrijdigheden tussen deze regels, prevaleren de eerder genoemden. Het is aan Helpdesk-CERT-SSH en de Helpdesk-abusegroep om te bepalen of gedrag al dan niet onder overtreding van de onderstaande gedragsregels valt.

3. Gedragsregels voor SSHnet-gebruikers

1. De internet aansluiting is voor persoonlijk gebruik van de aangesloten bewoner/gebruiker.

2. De gebruiker is persoonlijk verantwoordelijk voor al datgene dat via zijn computersysteem en/of
aansluiting gebeurt, ongeacht wie of wat de werkelijke veroorzaker is.

Hierbij wordt bijvoorbeeld gedacht aan:

- men mag geen mail services open hebben staan die misbruikt kunnen worden door derden om mail te versturen (d.w.z. geen open relay)
- men is verantwoordelijk voor ieder bestand en bericht dat via zijn computer en/of verbinding wordt aangeboden dan wel verstuurd, ongeacht de bron, ongeacht de methode
- men mag geen auteursrechtelijk beschermde gegevens aanbieden die niet zijn vrijgegeven door de rechthebbende
- men mag geen draadloze (o.a. wifi) verbindingen open hebben staan die voor anderen dan de gebruiker toegankelijk zijn.

3. Het is de gebruiker niet toegestaan zijn verbinding te gebruiken voor (semi)commerciële doeleinden en/of diensten of waarbij de computer en de verbinding van de gebruiker dienstbaar is aan (semi)commerciële doeleinden en/of diensten van derden via het SSHnet.

Hierbij wordt onder andere gedacht aan (deze lijst is niet uitputtend):

- het hosten van sites, services, en/of bestanden die horen bij een commerciële toepassing.
- zaken die niet in overeenstemming zijn met de doelstelling van de aangeboden verbindingen via de UU en Surfnet

4. Het is de gebruiker niet toegestaan om andere internetgebruikers, op welke manier dan ook, de toegang tot internet te ontzeggen, te beperken en/of te verhinderen.

Hierbij wordt onder andere gedacht aan (deze lijst is niet uitputtend):

- overmatig netwerkgebruik, bijvoorbeeld door teveel downloaden/uploaden en/of het draaien van web-, FTP-, p2p-services die (te) veel netwerkverkeer veroorzaken. In ieder geval is als overmatig te beschouwen: het overschrijden van de geldende limieten of het versturen of ontvangen van dusdanige grote hoeveelheden data dat er voor andere gebruikers verstoringen optreden.
- flush-pingen / flood-pingen
- het inbreken of misbruiken van computers en/of netwerkapparaten, of pogingen daartoe (al dan niet binnen het SSHnet)
- mailbomben, MSN/ICQ bombs en dergelijke hinderlijke activiteiten

5. De gebruiker zal geen 'disease', direct of indirect, gebruiken, (automatisch) in werking laten treden, versturen of aanbieden.

Hierbij wordt bij 'disease' onder andere gedacht aan (deze lijst is niet uitputtend):

- trojan horses, virussen, wormen, e.d.
- schadelijke executables (programma's).

6. Het is niet toegestaan om informatie te versturen of aan te bieden die in strijd is met algemeen geaccepteerde normen en waarden.

Hierbij onder andere gedacht aan:

- discriminerende en/of rascistische uitlatingen
- beledigende, en/of bedreigende informatie

7. Het is niet toegestaan te 'spammen' of derden lastig te vallen of te bedreigen vanaf een SSHnet aansluiting.

Hierbij wordt onder andere gedacht aan:

- het versturen van excessieve hoeveelheden e-mail/posts/berichten
- het lastig vallen van derden op websites, per mail, news, irc, icq, e.d.
- het posten in nieuwsgroepen van informatie die niet in die nieuwsgroep thuis hoort
- excessief kruisposten (het versturen van berichten naar teveel nieuwsgroepen of forumgroepen tegelijk)

8. Het is niet toegestaan een activiteiten te ondernemen en/of dingen na te laten die de integriteit van het SSHnet netwerk en/of de daarop aangeboden diensten in gevaar kunnen brengen.

Hierbij wordt onder andere gedacht aan:

- het uitlokken van een mail-, ping-, web-/news- posting-flood, DOS-aanval enzovoort
- het uitproberen van exploits, het (laten) uitvoeren van netwerk scans op andermans systemen, tenzij dit vooraf schriftelijk expliciet door de SSH is toegestaan aan de betrokkene
- het draaien van schadelijke en/of verkeerd geconfigureerde services
- het gebruik van systemen die zodanig geconfigureerd zijn, bijvoorbeeld door het niet op tijd installeren van patches voor software, dat derden gebruik kunnen maken van het systeem of dat het systeem geïnfecteerd kan raken met trojans, virussen of wormen die daarna met behulp van dat systeem verder kunnen verspreiden.

9. Het is niet toegestaan een SSHnet aansluiting op een locatie anders dan de kamer waar de aansluiting zich bevindt te gebruiken zonder schriftelijke toestemming van de SSH. Voor zelfstandige woningen geldt dat de aansluiting alleen binnen de aangesloten woning mag worden gebruikt.

Hierbij wordt onder andere gedacht aan:

- om een op het SSHnet aangesloten computer in een gemeenschappelijke ruimte te zetten.
- de aansluiting op het SSHnet te gebruiken om anderen via de computer/aansluiting van de gebruiker van internetdiensten te voorzien en/of de verbinding te delen met andere gebruikers.
- het draaien van inbelservices

10. Het is de gebruiker niet toegestaan om actief te zijn op een ander netwerkadres dan
door de netwerkbeheerder is toegestaan, dan wel door de DHCP-server is toegewezen.
Dit geldt zowel voor het zenden van netwerkpakkettenals voor het ontvangen ervan. De
gebruiker dient andermans privacy te respecteren.

Hierbij wordt onder andere gedacht aan:

- het zelf instellen van een IP-adres;
- het versturen van pakketten met als afzender-IP-adres, een adres dat niet overeenkomt met die van de daadwerkelijke afzender;
- sniffen, waarbij pakketten bedoeld voor een anders dan die van de gebruiker worden ontvangen.

4. Sancties

Bovenstaande regels worden door de SSH en Universiteit beschouwd als normen die een uitleg geven van de voorwaarden waaronder de toegang tot het netwerk wordt verleend. Ze zijn richtinggevend voor het afhandelen van misbruikgevallen en kunnen tot een besluit van de abusegroep leiden dat er maatregelen tegen de gebruiker genomen moeten worden.
Afhankelijk van de aard en de zwaarte van de overtreding volgt er eerst één mondelinge of schriftelijke waarschuwing. Bij herhaling of zware overtredingen volgen er onmiddellijke sancties.

Tot de mogelijke sancties behoren:

- het afsluiten voor bepaalde of onbepaalde tijd
- afsluiting waarbij heraansluiting mogelijk is na betaling van EUR 200,-.
- het verhalen van schade

Het is aan de abusegroep een passende maatregel te bepalen en op te leggen. Maatregelen waarbij heraansluitingskosten of schadevergoeding zullen worden gevraagd, zullen door de SSH worden behandeld.

5. Slotbepalingen

- De SSH kan deze gedragsregels te allen tijde wijzigen. De nieuwe gedragsregels gaan dan met onmiddellijke ingang in, en zullen bekend worden gemaakt op de SSHnet website.

- Ten behoeve van de gebruikers is er een klachtenreglement opgesteld. Hierin staat aangegeven hoe je een klacht kunt indienen over handelingen van de abusegroep. Nadien kan de gebruiker in beroep bij de SSH.

- In bijzondere gevallen kan de SSH, op schriftelijk verzoek van de gebruiker, afwijkingen toestaan op deze Policy. Deze toestemming moet schriftelijk en vooraf verleend zijn. Indien je denkt een hogere datalimiet en/of andere uitzonderingen nodig te hebben kun je een schriftelijk verzoek indienen bij de SSH.

Aan deze policy kunnen geen rechten worden ontleend.