# Model Acceptable Use Policy voor studenten

Modelreglement voor ICT- en internetgebruik voor studenten aan <NAAM_INSTELLING>


Auteur(s): Samenwerking tussen SURFibo en SURFnet



Versie: 4.0

Datum: 16 april 2013


Het SURF Informatie Beveiligers Overleg is ingesteld door het platform SURF ICT en Organisatie met als doelen het actief stimuleren van en richting geven aan informatiebeveiliging binnen het hoger onderwijs (universiteiten, hogescholen en universitair medische centra). Dat wordt bereikt door het bevorderen van de samenwerking tussen informatiebeveiligers en het leveren van praktisch bruikbare adviezen.

Voor meer informatie zie www.surfibo.nl

**Versiebeheer:**

| Versie | Datum | Korte beschrijving aanpassingen |
|---|---|---|
| 1.0 | November 2005 | Eerste versie |
| 2.0 | Augustus 2011 | Aanpassingen o.a. mbt. BYOD |
| 3.0 | November 2012 | Volledige revisie n.a.v. nieuwe wetgeving mei 2012:<br>- splitsing in model-AUP's voor studenten en werknemers<br>- AUP's ook in Engels beschikbaar<br>- Losse leidraden voor gebruik |
| 4.0 | April 2013 | Aanpassingen mbt vertrouwelijkheid, privacy en (intellectueel) eigendom (ihkv Cloudcomputing) |

**Samengesteld door:**

| Organisatie | | Toelichting |
|---|---|---|
| ICTrecht | ICTRECHT | Arnoud Engelfriet, juridisch advies<br>eindredactie versie 3.0<br>www.ictrecht.nl |
| SURFnet | SURF NET | Rogier Spoor, coördinatie<br>Evelijn Jeunink, juridisch advies<br>www.surfnet.nl |
| SURFibo | SURF Informatie Beveiligers Overleg | Bart van den Heuvel, coördinatie<br>Met dank aan diverse leden van SURFibo voor hun bijdragen in workshops en als reviewer<br>www.surfibo.nl |
| SCIRT | scirt forum for operational security | Met dank aan diverse leden van SCIRT voor hun bijdragen in workshops en als reviewer<br>www.surfnet.nl/nl/Thema/beveiliging/scirt/Pages/scirt.aspx |

**Bronvermelding:**

De ICT-reglementen voor werknemers en studenten van <NAAM_INSTELLING> zijn gebaseerd op Model reglementen voor het Hoger Onderwijs, een gezamenlijk product van SURFnet en SURFibo.

# Acceptable Use Policy voor studenten aan <NAAM_INSTELLING>

De NAAM_INSTELLING (hierna: de Instelling) biedt aan de eigen studenten en aan bezoekende studenten de mogelijkheid internet te gebruiken ten behoeve van de studie. Tevens word[t][en] aan studenten voor persoonlijk gebruik een instellingsgebonden mailbox [en mogelijkheden tot opslag van bestanden en persoonlijke studiegegevens] beschikbaar gesteld ten behoeve van de studie.

Aan het gebruik van deze faciliteiten zijn regels verbonden, in het kader van de goede gang van zaken in de gebouwen en op de terreinen van de Instelling.

## *Gebruik van faciliteiten*

Computer- en netwerkfaciliteiten (zoals openbare computers, draadloze en bedrade netwerkaansluitingen, e-mail en internettoegang, opslagcapaciteit, printers en elektronische leeromgevingen) worden aan de student beschikbaar gesteld ten behoeve van de studie, onder meer voor het kunnen maken van opdrachten, verslagen en scripties, het bijhouden van de studievoortgang, het raadplegen van bronnen en het communiceren met docenten en medestudenten.

Het gebruik van eigen apparatuur en toepassingen op de faciliteiten van de Instelling is toegestaan zolang dit gebruik voldoet aan de regels van dit Reglement. Het veranderen van instellingen in apparatuur en toepassingen beschikbaar gesteld door de Instelling is alleen toegestaan met aparte toestemming van het systeembeheer. Het aansluiten van eigen netwerkapparatuur waarmee de verbinding kan worden gedeeld met derden op de bedrade of draadloze netwerkaansluitingen is te allen tijde verboden[, behalve in de woonruimte van studenten].
[INDIEN EDUROAM] Dit Reglement geldt ook indien u als gast gebruik maakt van netwerkvoorzieningen van andere instellingen waarbij toegang wordt verkregen op basis van de inloggegevens van de eigen Instelling (Eduroam).

Bepaalde faciliteiten zijn alleen toegankelijk met behulp van een gebruikersnaam en [wachtwoord|authenticatiemiddel zoals smartcard of GSM]. Deze zijn persoonsgebonden en mogen niet met anderen worden gedeeld. Het systeembeheer kan nadere eisen stellen aan de kwaliteit van wachtwoorden en andere beveiligingsaspecten[, zoals nader geformuleerd in het Informatiebeveiligingsbeleid]. Bij een vermoeden van misbruik van een wachtwoord [of authenticatiemiddel] kan het systeembeheer per direct het betreffende account ontoegankelijk maken.

## *Intellectueel eigendom en vertrouwelijke informatie*

De student maakt geen inbreuk op de intellectuele eigendomsrechten van de Instelling en derden en respecteert de licentie afspraken zoals die van toepassing zijn binnen de Instelling.

[OPTIE: De zeggenschap over de informatie van de Instelling berust bij Instelling. De student heeft geen zelfstandige zeggenschap over de informatie behalve als hem dat expliciet is toegekend door de Instelling]

[OPTIE: Het is de student niet toegestaan om grote hoeveelheden artikelen uit de bestanden van de digitale bibliotheek te downloaden of substantiële delen van de bestanden of databases in de digitale bibliotheek systematisch te kopiëren.]

Indien de student in het kader van zijn studie of het uitvoeren van taken voor de Instelling toegang krijgt tot vertrouwelijke informatie of privacy gevoelige informatie waaronder persoonsgegevens, dient de student die informatie strikt vertrouwelijk te behandelen.
De student besteedt bijzondere aandacht aan het treffen van maatregelen zoals in dit Reglement genoemd, indien in het kader van het uitvoeren van deze taken de verwerking van vertrouwelijke informatie buiten de Instelling noodzakelijk is zoals via E-mail, in niet instellingsgebonden Cloud-toepassingen, op externe opslagmedia of eigen client-apparatuur (USB-apparaten, Tablets, etc.).

Indien de Instelling met betrekking tot het waarborgen van de vertrouwelijkheid en de intellectuele eigendomsrechten voorschriften heeft opgesteld dient de student deze stipt op te volgen.

## *Beveiliging door de Instelling én de student*

De Instelling neemt informatiebeveiliging serieus. Zij hanteert dan ook een streng beveiligingsbeleid en neemt adequate technische en organisatorische maatregelen om de infrastructuur te beveiligen tegen verlies, diefstal, criminele activiteiten, verlies van vertrouwelijkheid, schending van privacy-rechten en schending van intellectuele eigendomsrechten.

Natuurlijk is een perfecte beveiliging onmogelijk. Daarom verwacht de Instelling ook van studenten een proactieve houding en serieuze stappen om de eigen computer en andere apparatuur (zoals smartphones of tablets) adequaat te beveiligen. Zo is de student te allen tijde zelf verantwoordelijk voor het gebruik van de eigen apparatuur en de op deze apparatuur opgeslagen gegevens

[OPTIE: In het bijzonder dient de student indien met zijn apparatuur gebruikt wordt gemaakt van de instellingsfaciliteiten in het kader van beveiliging:

- deze apparatuur te voorzien van een adequate virusscanner en firewall;
- regelmatig reservekopieën te maken van alle relevante data en kopieën van instellingsdata veilig op te slaan;
- moeilijk te raden wachtwoorden te gebruiken en deze regelmatig te veranderen;
- deze apparatuur up-to-date te houden wat betreft software-instellingen;
- <ETC>]

[OPTIE Het systeembeheer zal een lijst publiceren met veiligheidsmaatregelen, welke regelmatig zal worden herzien. De student dient deze maatregelen stipt op te volgen.]

## *Privégebruik en overlast*

Beperkt privégebruik van de faciliteiten is toegestaan. Gebruik, privé of ten behoeve van studie, mag niet storend zijn voor de goede orde bij de Instelling en mag geen overlast veroorzaken bij anderen, inbreuk maken op rechten van de Instelling of derden of de integriteit en de veiligheid van het netwerk aantasten.

Onder storend en/of overlast veroorzakend gebruik wordt in ieder geval verstaan:

- het in openbare ruimtes raadplegen van internetdiensten met een pornografische, racistische, discriminerende, beledigende of aanstootgevende inhoud of het verzenden van berichten met een dergelijke inhoud;
- het verzenden van berichten met een (seksueel) intimiderende inhoud of van berichten die (kunnen) aanzetten tot discriminatie, haat en/of geweld;
- het versturen van berichten aan grote aantallen ontvangers tegelijk, het versturen van kettingbrieven of het verspreiden van kwaadaardige software zoals virussen, wormen, Trojaanse paarden en spyware;
- [filesharing- of streamingdiensten (zoals internetradio of Uitzendinggemist) te gebruiken wanneer dit overmatig veel dataverkeer genereert, zodanig dat het de beschikbaarheid van de faciliteiten in gevaar kan brengen;]
- [films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van enige illegale bron of wanneer de student weet/moet weten dat dit in strijd met auteursrechten is;]
- [films, muziek, software en overig auteursrechtelijk beschermd materiaal te verspreiden (uploaden) naar derden zonder toestemming van de rechthebbenden.]

Studenten die in hun woonruimte gebruik maken van een netwerkfaciliteit van de Instelling worden aldaar geen beperkingen opgelegd aan het gebruik, behoudens voor zover noodzakelijk om de integriteit en de veiligheid van het netwerk te kunnen bewaren, of om de gevolgen van congestie te beperken. Indien de Instelling ingrijpt om de gevolgen van congestie te beperken, zullen gelijke soorten verkeer gelijk worden behandeld. De overige bepalingen in deze AUP zijn onverkort van toepassing voor studenten-gebruikers die in hun woonruimte gebruik maken van een netwerkfaciliteit van de Instelling.

Het gebruik van computer- en netwerkfaciliteiten ten behoeve van commerciële activiteiten is uitsluitend toegestaan wanneer de Instelling hiervoor schriftelijk toestemming heeft verleend.

## *Monitoring door de Instelling*

Controle van gebruik van de faciliteiten vindt slechts plaats in het kader van handhaving van de regels uit dit Reglement ten behoeve van de goede orde op de Instelling en de bewaking van de integriteit en de veiligheid van het netwerk en de computerfaciliteiten

van de Instelling. Verboden gebruik van de faciliteiten wordt zo veel mogelijk langs technische weg onmogelijk gemaakt.

Ten behoeve van deze controle worden geautomatiseerd gegevens verzameld (gelogd). Deze gegevens zijn alleen toegankelijk voor de direct verantwoordelijke systeembeheerders en worden alleen in geanonimiseerde vorm aan overige beheerders en andere verantwoordelijken beschikbaar gesteld. Deze kunnen tot nadere technische maatregelen besluiten, zoals een blokkade van de toegang tot een bepaalde dienst of het beperken van de mogelijkheden van het apparaat in kwestie om het netwerk te kunnen gebruiken.

In het bijzonder kan bij overlast, veroorzaakt door apparatuur van studenten, worden overgegaan tot uitschakeling van de netwerktoegangsmogelijkheden. Indien mogelijk wordt de student vooraf gewaarschuwd, zodat hij de gelegenheid heeft de overlast te staken. Wanneer dit wegens de vereiste spoed niet voorafgaand aan het nemen van de maatregel mogelijk is, doet men zo snel mogelijk melding van de maatregel.

Bij vermoedens van overtreding van de regels kan controle worden uitgevoerd op het niveau van individuele verkeersgegevens van het gebruik van de faciliteiten. Slechts bij zwaarwegende redenen vindt controle op de inhoud plaats.

De Instelling houdt zich bij het controleren op het niveau van verkeersgegevens of de inhoud onverkort aan de Wet bescherming persoonsgegevens en andere relevante wet- en regelgeving. In het bijzonder beveiligt de Instelling de bij controle vastgelegde gegevens tegen ongeautoriseerde toegang en zijn personen met toegang daartoe contractueel verplicht tot geheimhouding.

### *Procedure bij gericht onderzoek*

Van gericht onderzoek is sprake wanneer verkeersgegevens of andere persoonsgegevens betreffende de student worden vastgelegd in het kader van een onderzoek naar aanleiding van een zwaarwegend vermoeden van een overtreding van dit Reglement door die student.

Gericht onderzoek vindt uitsluitend plaats na schriftelijke opdracht van de directeur van de faculteit, welke toestemming de redenen zal noemen waarom deze wordt verleend. Het College van Bestuur ontvangt een afschrift van deze opdracht en een vastlegging van de resultaten van het onderzoek.

Gericht onderzoek beperkt zich in eerste instantie tot verkeersgegevens van het gebruik van de faciliteiten. Als gericht onderzoek nader bewijs oplevert, kan de Instelling na aparte toestemming overgaan tot het kennisnemen van de inhoud van communicatie of opgeslagen bestanden. Indien het onderzoek geen aanleiding geeft tot verdere maatregelen wordt de vastlegging vernietigd.

Gericht onderzoek naar de beveiliging of integriteit van randapparatuur mag in afwijking hiervan door het systeembeheer worden uitgevoerd op basis van concrete aanwijzingen, zonder aparte toestemming. De resultaten van dit onderzoek worden alleen gedeeld met de student met het doel de beveiliging of integriteit van de randapparatuur te verbeteren. Bij herhaling zal de procedure uit het vorige lid worden gevolgd.

De student wordt zo spoedig mogelijk schriftelijk geïnformeerd door de directeur over de aanleiding, de uitvoering en het resultaat van het onderzoek. De student wordt in de gelegenheid gesteld uitleg te geven over de aangetroffen gegevens. Uitstel van het informeren mag alleen als informeren het onderzoek daadwerkelijk zou schaden.

Systeembeheerders verschaffen zich slechts toegang tot accounts of computers van de student als de student daarvoor zijn toestemming heeft gegeven. Toegang zonder deze toestemming is slechts toegestaan in dringende gevallen of bij een duidelijk vermoeden van schending van dit Reglement, zoals nader bepaald in dit artikel. De student zal in dat geval achteraf worden geïnformeerd.

### *Rechten van de student met betrekking tot persoonsgegevens*

De student kan zich tot het bestuur wenden met het verzoek om een volledig overzicht van zijn persoonsgegevens zoals door de Instelling verwerkt in het kader van dit Reglement. Aan een dergelijk verzoek wordt binnen vier weken voldaan.

De student kan het bestuur verzoeken zijn persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor het doel onvolledig of niet ter zake dienend zijn, dan wel in strijd met een wettelijk voorschrift zijn. Op een dergelijk verzoek wordt binnen vier weken gereageerd. Een weigering is met redenen omkleed. Een toegewezen verzoek zal zo spoedig mogelijk worden uitgevoerd.

De student kan verder verzet aantekenen tegen de verwerking van zijn persoonsgegevens in verband met zwaarwegende persoonlijke omstandigheden. Het bestuur oordeelt binnen vier weken na ontvangst van het verzet of dit gerechtvaardigd is. Indien het bestuur het verzet gerechtvaardigd acht, beëindigt zij terstond de verwerking.

### *Consequenties van overtreding*

Bij handelen in strijd met dit Reglement of de algemeen geldende wettelijke regels, kan het bestuur van de Instelling afhankelijk van de aard en de ernst van de overtreding disciplinaire maatregelen treffen.

[OPTIE A: aparte maatregelen] Hieronder vallen een waarschuwing, berisping, een tijdelijke afsluiting of beperking van de faciliteiten (maximaal een jaar) en in extreme gevallen een beëindiging van de inschrijving als student.

[OPTIE B: verwijzing] zoals nader bepaald in de Regeling Disciplinaire maatregelen van de Instelling.

[VERPLICHT bij A of B] Disciplinaire maatregelen (behalve een waarschuwing) kunnen niet worden getroffen enkel op basis van een langs geautomatiseerde weg uitgevoerde verwerking van persoonsgegevens, zoals een constatering van een automatisch filter of blokkade. Voorts worden geen disciplinaire maatregelen getroffen zonder dat de student gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.

In afwijking van het voorgaande is het mogelijk dat de Instelling bij (geautomatiseerde) constatering van overlast een tijdelijke blokkade van de betreffende faciliteit invoert. Deze blokkade zal maximaal een week worden gehandhaafd of korter als de oorzaak naar tevredenheid van het systeembeheer is weggenomen. Indien na een week geen verbetering is geconstateerd door het systeembeheer, kan het systeembeheer besluiten tot een langere blokkade. Bij herhaling van de oorzaak kunnen disciplinaire maatregelen worden genomen.

## *Slotbepalingen*

Dit Reglement kan door het bestuur worden herzien. Wijzigingen worden alleen bij het begin van een collegejaar doorgevoerd, behalve in dringende gevallen of wanneer de Instelling door omstandigheden van buitenaf gedwongen is tot een snellere invoering.

Wijzigingen worden alleen ingevoerd nadat de instellingsmedezeggenschapsraad om voorafgaand advies is gevraagd. Het bestuur zal feedback van studenten in overweging nemen alvorens de wijzigingen in te voeren.

In gevallen waarin dit Reglement niet voorziet, beslist het College van Bestuur.