Leidraad Model Acceptable Use Policy voor studenten

Een leidraad bij het gebruik van het document “Model Acceptable Use policy voor studenten”

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 AUP, zonder Leidraad
2.0	Augustus 2011	Aanpassingen o.a. mbt. BYOD, zonder Leidraad
3.0	November 2012	Volledige revisie n.a.v. nieuwe wetgeving mei 2012: - splitsing in model-AUP's voor studenten en werknemers - AUP's ook in Engels beschikbaar - 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 eindredactie versie 3.0 www.ictrecht.nl
SURFnet	SURF NET	Rogier Spoor, coördinatie Evelijn Jeunink, juridisch advies www.surfnet.nl
SURFibo	SURF Informatie Beveiligers Overleg	Bart van den Heuvel, coördinatie Met dank aan diverse leden van SURFibo voor hun bijdragen in workshops en als reviewer www.surfibo.nl
SCIRT	scirt forum for operational security	Met dank aan diverse leden van SCIRT voor hun bijdragen in workshops en als reviewer 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.

Leidraad AUP voor studenten

Deze leidraad dient als aanvulling op de Acceptable Use Policy voor studenten aan bij SURF aangesloten instellingen. De AUP is opgezet als een algemeen bruikbaar document, met optionele elementen die een instelling wel of niet kan kiezen. Voor medewerkers is een apart modelreglement opgesteld.

Er is gekozen voor zo veel mogelijk klare taal in de hoop dat studenten deze dan lezen en ter harte nemen. Verder worden geen details opgenomen zoals hoe lang wachtwoorden moeten zijn en dat men de eigen gegevens moet backuppen. Dit spreekt in principe voor zich; waar behoefte is aan aanvullende duidelijke tips kan beter met een apart document worden gewerkt.

Het modelreglement moet door de instelling worden aangepast aan de eigen werkwijze en wensen, binnen de wettelijke grenzen uiteraard. Denk hierbij ook aan terminologie (systeembeheer/IT-beheer/ICT-beheer?), de bestuursstructuur, referenties aan vigerende reglementen, sanctiebeleid, etc.

Hoewel in principe alles aan te passen is, wordt aanbevolen om alleen de opties te wijzigen die expliciet als zodanig zijn gemarkeerd met vierkante haken [].

Communicatie

Daarna moet het document worden bekend gemaakt aan de studenten. Te denken valt aan publicatie op de internetsite van de instelling, met een prominente hyperlink bij het aanmeldproces.
Goede communicatie over het reglement is niet alleen essentieel voor de feitelijke juridische draagkracht, maar ook een uitstekend middel om extra aandacht te vragen voor specifieke instellingssituaties of de actualiteit. In deze communicatie kunnen bv. referenties opgenomen worden aan overige reglementen of aandachtsgebieden als het van toepassing zijn van de reglementen op instellingsformatie, privacy en Bring Your Own Device kunnen expliciet toegelicht worden.

Dergelijke informatie en bv. aanvullende informatie over de werkwijze bij waarschuwingen en sancties kan ook in een brochure en/of in een inleiding op een webpagina over het reglement gecommuniceerd worden.

Aanhef

De aanhef van de AUP schetst de kaders en de wettelijke grenzen. De insteek is die van “faciliteiten zijn er voor de studie”, en “handhaving gebeurt ten behoeve van de goede orde” (wat de bevoegdheid dus baseert op de Wet op het Hoger Onderwijs). Daarmee kunnen de regels eenzijdig worden opgelegd.
Bij het formuleren van het reglement is uitgegaan van de algemene thema’s beschikbaarheid, vertrouwelijkheid, privacy en (intellectueel) eigendom.

Gebruik van faciliteiten

In dit algemene artikel wordt nader uitgewerkt hoe het zit met het gebruik van de faciliteiten. Deze term verwijst zowel naar bv. computers van de instelling in de bibliotheek als naar netwerkaansluitingen of draadloze netwerken aangeboden aan studenten en gasten.

De faciliteiten worden aangeboden voor de studie, wat onderbouwd wordt met enkele voorbeelden (maken verslagen, communiceren met docenten). Met deze insteek wordt de problematiek van netneutraliteit zo veel mogelijk vermeden, maar het is onzeker of dit 100% waterdicht is. Wanneer sprake is van “aanbieden van internettoegang” valt men onder netneutraliteit. Die term wordt daarom zo veel mogelijk vermeden en er wordt aansluiting gezocht bij de uitzondering voor werknemers die het “bedrijfsmiddel internet” krijgen en daarmee buiten netneutraliteit vallen. Studenten krijgen de studiefaciliteit internet onder andere om toegang te hebben tot openbare bronnen van belang voor de studie.

Intellectueel eigendom en vertrouwelijke informatie

Dit artikel gaat specifiek in op de wijze waarop de instelling verwacht dat haar studenten omgaan met informatie die zij verwerken (zelf genereren, bewerken, lezen, kopiëren, verzenden, publiceren, etc. etc.). Het gaat daarbij dus om de algemene uitgangspunten vertrouwelijkheid, privacy en (intellectueel) eigendom.

Een specifiek artikel is opgenomen over de zeggenschap van informatie. Afspraken daarover kunnen al in een ander reglement opgenomen zijn, maar als dat niet het geval is kan er in dit reglement specifiek aandacht aan worden besteed.

Een specifieke optie is opgenomen over opvragen van documenten uit digitale bibliotheken. Dit is opgenomen om de organisatie te beschermen tegen auteursrechtenclaims en wanprestatie naar artikelleveranciers toe. Deze verbieden namelijk normaal gesproken het genoemde veelvuldig opvragen van artikelen. Als een instelling hier geen specifieke afspraken over heeft, of als gebruik van de bibliotheek met aparte eigen regels komt, dan is dit specifieke artikel niet nodig.

Verder behandelt dit artikel de specifieke situaties mbt informatie die onder verantwoordelijkheid van de student beschikbaar komt op ICT-voorzieningen of op andere wijze, waarbij de instelling geen directie zeggenschap heeft over die middelen. (Cloudvoorzieningen, Tablets, USB-devices etc.).

Beveiliging door de instelling én de student

Het beveiligingsbeleid van de instelling is ook deel van de AUP, zowel naar de student toe (die dient te beveiligen) als ten behoeve van de student (die mag een veilige omgeving verwachten). Hier is het moeilijk veel algemeens te zeggen, vandaar dat volstaan wordt met enkele generieke zinnen en een opsomming van mogelijke specifieke aandachtspunten.

Het wordt afgeraden om hier hele pagina's aan te besteden, aangezien die waarschijnlijk snel achterhaald zijn en dat problematisch is omdat het reglement niet zomaar gewijzigd

mag worden. Aanbevolen wordt om *best practices* op dit gebied als apart document te publiceren. Vandaar de optie om óf een lijst op te nemen óf te verwijzen naar de lijst die systeembeheer zal publiceren.

Privégebruik en overlast

Gekozen is voor een beperkte toestemming voor privégebruik, vergelijkbaar met de optie die voor werknemers beschikbaar is. Toegevoegd is “integriteit en veiligheid van het netwerk aantast”, afkomstig uit de netneutraliteitswet. Deze term zal nog enkele malen terugkomen. Let wel dat het moet gaan om de *technische* integriteit en veiligheid. Een opruiende mail brengt de veiligheid van het netwerk niet in gevaar bijvoorbeeld, net zo min als een Bittorrent client. De wet overtreden is geen technisch integriteitsprobleem.

Voor de duidelijkheid zijn een aantal zaken opgenomen die eigenlijk altijd als storend of overlastgevend worden gezien. Denk aan het bekijken van porno of het versturen van virussen.

Discutabel is of filesharing en streaming op de lijst hoort. Dit specifiek blokkeren botst namelijk met netneutraliteit, aangezien daar alleen op basis van “gelijke soorten verkeer gelijk behandelen” mag worden gewerkt.

Een optie is opgenomen voor streaming en downloaden wanneer dit overmatig veel dataverkeer gebruikt. Deze optie is eigenlijk alleen redelijkerwijs te handhaven als het kenbaar is voor de student dát hij zo veel dataverkeer genereert. De instelling zou bij de keuze voor deze optie dus een specifieke waarde moeten opnemen en een dataverkeermeter moeten bieden, of bijvoorbeeld eerst een waarschuwingsmailtje sturen met “u zit bijna aan wat wij overmatig veel vinden”. Zie hiervoor ook de opmerkingen bij “Consequenties van overtreding” verderop.

Tevens discutabel is de optie van het downloaden uit enig illegale bron. Dit is namelijk strikt gesproken legaal onder de huidige rechtspraak. Bovendien is de instelling niet aansprakelijk voor schending auteursrechten door studenten via de ICT-faciliteiten. Zij is zelfs niet verplicht tot filteren of blokkeren van studenten over te gaan zonder tussenkomst van de rechter. Dit geldt zowel bij uploaden als bij downloaden.

Als de instelling een proactieve uitstraling ten aanzien van auteursrechten wenst aan te nemen, kunnen de opties rond up- en downloaden worden opgenomen. Wanneer deze optie wordt gehandhaafd, kunnen rechthebbenden (zoals BREIN of Amerikaanse filmmaatschappijen) wijzen op deze optie om alsnog afsluiting of andere maatregelen tegen de student te eisen. De instelling verplicht zich dus tot handhaving bij het opnemen van deze clausule.

In het specifieke geval van internettoegang in de privé woonruimte is netneutraliteit onvermijdelijk. Hier mag dus niet worden gefilterd of geblokkeerd, behalve voor zover in de netneutraliteitswet is bepaald. Hierover is een apart artikel opgenomen.

Monitoring door de instelling

De instelling heeft het recht het gebruik van de faciliteiten te monitoren en maatregelen te nemen. Ook hier weer geldt dat dit recht beperkt moet zijn tot de goede orde en de integriteit en veiligheid van het netwerk.

De insteek is privacyvriendelijk: er wordt in beginsel alleen geautomatiseerd gelogd en er worden maatregelen genomen zoals toegangsblokkades en het beperken van de mogelijkheden van apparaten (bv. via MAC adres blokkeren of routeren naar buiten het eigen netwerk tegengaan). Pas bij concrete aanwijzingen kan een individuele student gemonitord worden of zijn privébestanden (zoals mailboxen) geraadpleegd.

Daarbij is het van belang om te bepalen op welk niveau welke maatregelen worden genomen. Zodra wordt gemonitord of gelogd op het niveau van verkeersgegevens of persoonsgegevens, gelden de wettelijke regels en beperkingen uit de Wet bescherming persoonsgegevens (Wbp). Wanneer inhoud wordt gelezen door mensen, is bijvoorbeeld altijd de Wbp van toepassing. Wordt vastgelegd hoe vaak student X mailt, dan geldt ook de Wbp.

Voor malware is een specifieke optie opgenomen, gebaseerd wederom op de netneutraliteitswet. Deze bepaalt dat blokkades en filteren bij malware toegestaan is, maar dat de abonnee (de student) eerst gewaarschuwd moet worden en zelf een mogelijkheid krijgt om maatregelen te nemen, tenzij “dit wegens de vereiste spoed niet voorafgaand aan het nemen van de maatregel mogelijk is.” Een volautomatisch filter dat een student afsluit omdat uitgaand malafide verkeer wordt gesignaleerd, is dus niet mogelijk behalve bij zeer ernstige kwaadaardige virussen.

Procedure bij gericht onderzoek

Desgewenst kan een specifieke escalatieprocedure worden toegevoegd. Deze is hier redelijk streng ingezet: voor elke inspectie van bestanden is toestemming van de faculteitsdirecteur nodig, met informatieplicht naar het College van Bestuur. Dit is niet de enige wettelijke optie, men kan de bevoegdheid ook bij het CvB direct leggen.

Rechten van de student met betrekking tot persoonsgegevens

Dit artikel werkt de Wet bescherming persoonsgegevens uit in de specifieke situaties die dit reglement mogelijk maakt. De termijnen en grenzen zijn gebaseerd op de wet en kunnen dus niet zomaar worden verlengd. Aanpassingen in het voordeel van de student mogen natuurlijk wel.

Consequenties van overtreding

Een reglement zonder consequenties is van weinig waarde. Daarom biedt dit artikel enkele opties om vast te leggen wat er gebeurt bij handelen in strijd met het reglement. Volgens de WHO mag men overgaan tot een tijdelijke afsluiting of beperking voor maximaal een jaar, en in ernstige gevallen een beëindiging van de inschrijving. Een waarschuwing of berisping mag altijd, want deze hebben formeel geen betekenis.

Als de instelling al een reglement heeft over disciplinaire maatregelen tegen studenten dan kan ook daarnaar verwezen worden. Zo hoeft men niet opnieuw het wiel uit te vinden.

TIP: Afhankelijk van de gekozen detaillering in dit reglement en eventuele andere instellingsreglementen kan het voor de student soms onduidelijk zijn wanneer er sprake is van een overtreding. Bepaald gedrag kan onbewust zijn, bv door toedoen van een virus of een foutieve instelling in de software, of het gevolg van het feit dat een medewerker bv. niet in kan schatten wanneer gebruik “overmatig” is. In dergelijke gevallen kan het raadzaam zijn, om in eerste instantie een waarschuwing te geven waarbij expliciet wordt aangegeven voor welk gedrag de waarschuwing geldt en wat de consequenties zijn van een eventuele herhaling. De student kan dan reageren op het geconstateerde en de instelling kan een dossier opbouwen. Een dergelijke werkwijze kan in een brochure en/of in een inleiding op een webpagina over het reglement gecommuniceerd worden.

De laatste twee leden volgen uit de Wet bescherming persoonsgegevens; het is wettelijk niet toegestaan mensen een disciplinaire maatregel op te leggen enkel op basis van een geautomatiseerd proces. Iemand automatisch schorsen omdat een filter een spamdetectie deed, is dus bijvoorbeeld onmogelijk. Een gesprek op basis van het filter en daarna een besluit tot schorsing mag natuurlijk wel.

Dit betekent concreet dat het *niet* toegestaan is om bij geconstateerde overlast per direct een computer van het netwerk te weren totdat de student zich meldt. Het beheer *moet* eerst de student informeren, tenzij “dit wegens de vereiste spoed niet voorafgaand aan het nemen van de maatregel mogelijk is” zoals het in de wet staat. Oftewel het is volstrekt onmogelijk om eerst contact op te nemen. “Volstrekt onmogelijk” gaat verder dan “dat duurt mij te lang”; het contact moet onmogelijk zijn.

Een optie die binnen de wettelijke kaders wel haalbaar moet zijn is een tijdelijke technische blokkade van een faciliteit (zoals internettoegang) mits deze proportioneel is gezien de overtreding en er altijd een mogelijkheid van bezwaar is. Daarom is opgenomen dat men maximaal een week mag worden geweerd door een automatisch proces, waarna óf de blokkade er weer vanaf gaat óf een mens besluit dat de blokkade gehandhaafd moet worden omdat het contact met de student nog steeds volstrekt onmogelijk is.

Slotbepalingen

Als afsluiting wordt nog gesteld dat het reglement kan worden aangepast. Dit mag in principe eens per collegejaar, het begin daarvan lijkt logisch. In dringende gevallen (of als bv. De wet of rechter dat bepaalt) mag het natuurlijk sneller.

De WHO bepaalt dat de instellingsmedezeggenschapsraad (MR) om voorafgaand advies moet worden gevraagd. Als geste is toegevoegd dat feedback van studenten mee zal worden genomen. Dit hoeft niet (kan al via de MR) maar wie weet wat een slimme student zelf nog inbrengt.

Uiteraard dient er over aanpassingen in het reglement duidelijk gecommuniceerd te worden. Zie hiervoor de paragraaf “communicatie” in de inleiding van deze leidraad.

Het verdient aanbeveling ook oude versies van het reglement beschikbaar te houden, bijvoorbeeld via het intranet

Tenslotte wordt aangegeven waar de beslissingsbevoegdheid ligt, mocht het reglement in enige situatie niet voorzien.