Leidraad Model Acceptable Use Policy voor werknemers

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

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 bij het Modelreglement voor ICT- en internetgebruik voor werknemers

Deze leidraad dient als aanvulling op het Modelreglement voor ICT- en internetgebruik voor werknemers van bij SURF aangesloten instellingen (voor studenten is een apart modelreglement opgesteld). Werknemers zijn alle personen die een arbeidsovereenkomst hebben met de instelling, ongeacht of deze tijdelijk of onbepaalde tijd is, nul- of meeruren is, via een uitzendconstructie loopt dan wel of zij onder een CAO vallen. Gasten zijn dus uitgesloten, maar vrijwillige tijdelijke krachten vallen er wel onder.

Deze leidraad geeft toelichting voor de beleidsbepalers in de instelling en is niet bedoeld voor eindgebruikers. Het modelreglement is opgezet als een algemeen bruikbaar document, met optionele elementen die een instelling wel of niet kan kiezen. Sommige keuzes zijn zonder meer mogelijk, andere hebben de nodige implicaties. Zo vereist de optie voor persoonsgericht monitoren een toestemming van het medezeggenschapsorgaan van de instelling alvorens het reglement mag worden ingevoerd.

Het modelreglement moet door de instelling worden aangepast aan de eigen werkwijze en wensen, binnen de wettelijke grenzen uiteraard. Diverse veel voorkomende opties zijn via vierkante haken [] aangegeven. Denk hierbij ook aan terminologie (systeembeheer/IT-beheer/ICT-beheer?), de bestuursstructuur, referenties aan vigerende reglementen, sanctiebeleid, etc.

Communicatie

Daarna moet het document worden bekend gemaakt aan de werknemers. 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 Cloudgebruik en bij Social Media 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.

Nieuwe werknemers dienen een exemplaar uitgereikt te krijgen of gewezen te worden op de vindplaats, bv. het personeelshandboek of het intranet.

Introductie

Het reglement begint met een introductie die de achtergronden en de wettelijke basis vastlegt. Zo is voor iedereen duidelijk waar het reglement vandaan komt.

Basis voor het reglement

Een reglement zoals dit dient een wettelijke basis te hebben. Die is er in arbeidsverhoudingen: art. 7:611 BW biedt de werkgever de optie om regels te stellen

over de manier waarop het werk wordt uitgevoerd en hoe de goede orde op de werkvloer moet worden bewaard. Dit mag eenzijdig; de werknemer hoeft dus niet akkoord te gaan met die regels, hij is er gewoon aan gebonden. Natuurlijk moet de werkgever zich als een goed werkgever gedragen; hij mag niet zomaar alles opleggen.

Naast deze wettelijke grondslag kan de CAO of een statuut van de instelling een basis bieden om regels te stellen. Als dat zo is, kunnen die in de tweede introductiezin worden genoemd.

Een reglement heeft pas waarde indien het bij de doelgroep bekend is. Een communicatieplan moet dus onderdeel vormen van het proces om een reglement op te stellen en mat name ook om het vast te stellen. Hiervoor ligt aansluiting bij de reguliere communicatiekanalen voor de hand. Overwogen kan worden om een specifieke campagne op te starten.

Indien social media

Voor steeds meer instellingen is social media een punt van zorg. Wat doen werknemers daar allemaal, en straalt dat niet op ons af? Vandaar dat in het model een optie is opgenomen om hier regels te stellen. Indien dat het geval is, moet in de introductie hiernaar verwezen worden. Het is namelijk een erg nieuw onderwerp en dus verdient het aparte aandacht.

Instemming Medezeggenschapsorgaan

De Wet op de Ondernemingsraden bepaalt dat het medezeggenschapsorgaan van een bedrijf of instelling instemmingsrecht heeft voor alle regelingen die leiden tot een verwerking van persoonsgegevens en/of de controle op gedrag of prestaties van werknemers. De Wet op het Hoger Onderwijs regelt ook instemmingsrecht, eventueel via een CAO of nadere interne afspraak. Om verwarring over terminologie te voorkomen, wordt in het modelreglement gesproken van 'medezeggenschapsorgaan'. Aanbevolen wordt deze term te vervangen door de in de organisatie daadwerkelijk geldende term.

Nadat de vereiste instemming is verkregen, kan de datum daarvan worden ingevuld in de introductie. Dit laat naar de werknemers zien dat hieraan gedacht is.

Artikel 1. Uitgangspunten

Het reglement opent met een eerste artikel dat de uitgangspunten formuleert. Bij het formuleren van deze uitgangspunten is uitgegaan van de algemene thema's beschikbaarheid, vertrouwelijkheid, privacy en (intellectueel) eigendom. Allereerst worden de doelen genoemd die het uitgangspunt vormen van het reglement. Dit is belangrijk, omdat deze doelen bepalen of een monitoringsactie of een sanctie gerechtvaardigd zijn. Zou bijvoorbeeld het doel “voorkomen van negatieve publiciteit” niet worden genoemd, dan kan de instelling een werknemer die negatieve publiciteit veroorzaakt door een bijzonder gebruik van de ICT-bedrijfsmiddelen niet aanspreken.

Omgekeerd betekent het ook dat de instelling expliciet moet zijn over haar doelen. Zo zal niet iedere instelling “voorkomen van negatieve publiciteit” willen vermelden als doel, omdat dit vragen oproept bij werknemers. Mag men dan niets kritisch meer zeggen op

internet? Echter, door het doel niet te noemen is tevens de mogelijkheid ontvallen om dit te doen. Men mag niet zeggen te monitoren voor beveiligingsdoeleinden en daarna alsnog de werknemer aanspreken bij een relletje veroorzaakt door een kritische opmerking.

Het volgende punt is hoe ruimhartig de werkgever wil zijn bij het privé internetten. Hiervoor zijn drie opties opgenomen, van zeer ruim tot zeer beperkt. Deze opties zijn met name van belang wanneer het gaat om het mogen ingrijpen of beperken van de mogelijkheden voor privégebruik. Opgemerkt zij nog dat het wettelijk niet toegestaan is om *ieder* privégebruik te verbieden.

Omdat voor studenten een aparte wettelijke regeling geldt (met onder omstandigheden een verplichting tot ongefilterd/netneutraal aanbieden van internet) is het reglement niet op studenten van toepassing. Of men gasten ook aan dit reglement wil houden, is een keuze. Het is niet verplicht.

Artikel 2. Intellectueel eigendom en vertrouwelijke informatie

Artikel 2 gaat specifiek in op de wijze waarop de instelling verwacht dat haar werknemers 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.

Ook aanvullend is een specifiek artikel opgenomen over het 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, dan is dit specifieke artikel niet nodig.

Verder behandelt artikel 2 de specifieke situaties mbt informatie die onder verantwoordelijkheid van de werknemer beschikbaar komt op ICT-voorzieningen of op andere wijze, waarbij de instelling geen directie zeggenschap heeft over die middelen. (Cloudvoorzieningen, Tablets, USB-devices etc.).

Tenslotte wordt specifiek aandacht gevraagd voor de bijzondere rol van IT-beheerders.

Artikel 3. Gebruik van computer- en netwerkfaciliteiten

Artikel 3 werkt de uitgangspunten nader uit voor de computer- en netwerkfaciliteiten. Hierbij duiken specifieke zaken op zoals *Bring your own device* (BYOD) die wel of niet kunnen worden toegestaan op voorhand, en het al dan niet moeten gebruiken van de ELO (zoals Blackboard) van de instelling om lesmateriaal te beschikbaar te stellen.

Een optie is opgenomen voor het opslaan van privébestanden of -informatie op systemen van de instelling. Wie geen streng uitgangspunt kiest, zal moeten tolereren dat mensen privébestanden opslaan op de systemen van de instelling. Wel is men natuurlijk niet gehouden deze te backuppen en daarmee ook niet om ze te restoren.

Wie wel streng is, kan echter nog steeds niet zomaar schijven doorzoeken op mogelijke privébestanden (of bestanden die de wet schenden). Er zal nog steeds een gegronde aanleiding moeten zijn.

Artikel 4. Gebruik van e-mail en andere ICT-communicatiemiddelen

Artikel 4 werkt de uitgangspunten voor e-mail en andere ICT-communicatiemiddelen nader uit. Hier worden enkele aanvullende specifieke verboden gesteld (zoals spammen of verspreiden van porno). De algemene regel van privacy op het werk gelden ook bij de zakelijke mailbox. De werknemer heeft (binnen het algemene kader en een specifiek e-mailkader) enige vrijheid voor privégebruik. Deze vrijheid mag niet zomaar worden beknot door bijvoorbeeld structureel monitoren.

Wanneer de werkgever streng is over privégebruik, is aan te bevelen om e-mail alleen toe te laten via een externe webmaildienst. Zo is het eenvoudig te rechtvaardigen dat de mailbox van het werk ook écht alleen werkzaken behoort te bevatten, en kan er dus eerder in deze mailbox worden gekeken bij bijvoorbeeld ziekte.

Het is ook mogelijk om privégebruik van de zakelijke mailbox toe te staan, en deze dan te monitoren op bv. het lekken van bedrijfsgeheimen. Dit monitoren en inzien van mailverkeer of mailboxen is later geregeld in artikel 7 en verder. Dit is belangrijk, want voor inzage van mailboxen en mailverkeer gelden strenge regels.

Artikel 5. Gebruik van internet

Artikel 5 werkt de uitgangspunten nader uit voor internettoegang. Wederom worden aanvullende regels gesteld, welke met name zijn gericht op overlast voorkómen.

Artikel 6. Social media

Wanneer een instelling het gebruik van social media wil reguleren, biedt artikel 6 een aantal opties. De instelling kan streng zijn, wat inhoudt dat men eigenlijk alleen onder de eigen naam maar zonder vermelding van de positie bij de instelling actief mag zijn op deze media.

Een minder strenge instelling moedigt het gebruik van social media juist aan en stelt randvoorwaarden.

Optioneel kan men nog een verbod opnemen op onderhouden van contacten met studenten/scholieren.

De modelregels over social media betreffen met name hoe de werknemer zich moet gedragen. Dit raakt aan integriteit en communicatie, en minder aan ICT als zodanig of de beveiliging daarvan. Een organisatie kan er dus voor kiezen deze regels niet in het ICT-gebruiksreglement op te nemen maar in een integriteitsverklaring of set ethische regels op te nemen.

Artikel 7. Monitoring en controle

Artikel 7 stelt enkele algemene regels over monitoring en controle. Het uitgangspunt is algemene monitoring (herkennen en blokkeren van overlastgevende sites) en automatische maatregelen (het weigeren af te leveren van als spam aangemerkte mail) zonder dat men werknemers direct aanspreekt.

Het is mogelijk om ook individueel te monitoren. Hierbij hoort in eerste instantie het controleren op verkeersgegevens (wie mailt met wie, welke sites worden bezocht) en pas bij zwaarwegende gevallen ook de inhoud van communicatie. Dit wordt nader in artikel 8 uitgewerkt.

Sommige organisaties willen het ICT-gebruik betrekken in de individuele beoordelingen (beoordelingsgesprekken) van werknemers. Men zou een werknemer zo een slechtere beoordeling kunnen geven als deze veel privé internet, bijvoorbeeld. Hoewel dit legaal is, wordt *dringend afgeraden* om dit in het ICT-reglement op te nemen. Een dergelijke onverwachte en ingrijpende maatregel hoort niet thuis in een reglement als dit. Dit dient expliciet en apart te worden geregeld, het liefst in de bestaande regeling op het gebied van personeelsbeoordeling.

Artikel 8. Procedure bij individuele controle

Artikel 8 werkt artikel 7 nader uit en bevat enkele belangrijke waarborgen om het proces van individuele (persoonsgerichte) controle zorgvuldig uit te voeren. De keuzes zijn redelijk arbitrair, bijvoorbeeld wanneer de directeur en wanneer het bestuur een stap moet nemen. Het uitwerken van de eigen keuzes is wél belangrijk.

Artikel 9. Rechten van de werknemer

Artikel 9 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 werknemer mogen natuurlijk wel.

Artikel 10. Consequenties van overtreding

Een reglement zonder consequenties is van weinig waarde. Daarom biedt artikel 10 enkele opties om vast te leggen wat er gebeurt bij handelen in strijd met het reglement. Het is belangrijk duidelijk kenbaar te maken wat de sancties zijn, omdat ze anders eerder door de rechter ongedaan gemaakt kunnen worden of tot verplichtingen tot betalen van ontslagvergoedingen voor de werkgever kunnen leiden. Natuurlijk moeten de sancties ook inhoudelijk redelijk en passend zijn; ontslag op staande voet vanwege één pikant mailtje is onmogelijk.

Opties A en B bieden grondslag voor daadwerkelijke arbeidsrechtelijke stappen, waarbij optie A zélf opties noemt en B verwijst naar de reeds geldende regeling op dit gebied. (De naam moet uiteraard worden aangepast). Voordeel van het laatste is dat men niet apart hoeft uit te werken hoe en welke disciplinaire maatregelen kunnen worden opgelegd. Bij optie A moet dit wel.

Indien optie A of B wordt gekozen, is artikel 10.2 verplicht. Dit artikel volgt 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. Ook toegestaan is het geven van een waarschuwing, dit regelt 10.3.

TIP: Afhankelijk van de gekozen detaillering in dit reglement en eventuele andere instellingsreglementen kan het voor de werknemer 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, ook bij optie A of B, 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 werknemer 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.

Bij optie C wordt niet meer bepaald dan dat er een stevig gesprek zal komen en maatregelen worden genomen zoals het afsluiten van de internetverbinding. Dit is eenvoudig in te voeren en kan in de praktijk zeer effectief zijn, maar het maakt het onmogelijk iemand te ontslaan op grond van overtreding van het reglement.

Artikel 11. Slotbepaling

Als slotbepaling is opgenomen dat de regeling jaarlijks wordt geëvalueerd. Deze periode is natuurlijk arbitrair maar een kortere periode levert al snel discussies op.

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.