Integriteits- en gedragscode ICT-functionarissen UM

Datum 1ste versie	Registratie nummer	Auteur	Wijzigingsbeheer
20 oktober 2004	**ICTS/IS-2006-00124**	**Bart van den Heuvel, ICTS**	**Central Information Security Officer**
STATUS: Definitieve Werkinstructie			
Verspreiding document	**Concept: BJZ, directie ICTS, DO-ICT** **Besluitvorming: CBB, portefeuillehouder ICT,** **Uitvoer: Directies die werkinstructie van toepassing verklaren/ P-functionarissen** **Ter kennisname: LO-lijst**		

Versie	Datum	Omschrijving wijziging
0.1	**20 okt. 2004**	**1ste versie, voor commentaar BJZ**
0.2	**26 nov. 2004**	**Aangepast naar aanleiding van commentaar BJZ**
0.3	**13 jan. 2005**	**Aangepast naar aanleiding van commentaar BJZ, toelichting naar bijlage**
1.0	**31 jan. 2005**	**1-ste operationele versie, goedgekeurd door Directie en Dienstraad**
1.1	**8 maart 2005**	**taalcorrecties**
2.0	**1 sept. 2005**	**Aangepast concept om code UM-breed te kunnen toepassen**
3.0	**6 april 2006**	**Aangepast als werkinstructie en Campus- en CAO-aanpassing**
3.1	**27 sept 2006**	**1.2 aangepast n.a.v. LO-opmerking mbt mandatenregeling**

DEFINITIES:

Informatieverwerking en informatiesystemen:
Elke vorm van het verwerken of gebruiken van elke vorm van informatie en van informatiesystemen.
Voorbeelden van verwerken:

- het beschikbaar hebben of verkrijgen;
- het lezen, verveelvuldigen, of verwijderen;
- het verspreiden in welke vorm dan ook (digitaal, op papier, gesproken woord, etc.).

Voorbeelden van informatie en informatiesystemen:

- digitale gegevens, systeemprogrammatuur en applicatieprogrammatuur;
- gesproken woord, geschriften, beeld- en geluidsmateriaal;
- hulpmiddelen in welke vorm dan ook (computers, telefoons, printers, faxen, kopieermachines, draagbare apparatuur, etc.).

Incident m.b.t. informatie(beveiliging) en het gebruik van informatiesystemen:
Elke (dreiging tot) inbreuk op de vertrouwelijkheid, integriteit en beschikbaarheid alsmede (dreiging van) elke vorm van niet toegestaan gebruik van informatie en informatiesystemen, direct of indirect vallende onder het beheerdomein van de ICT-functionaris of de Universiteit Maastricht.

Niet toegestaan gebruik:
Elke vorm van gebruik van informatie en informatiesystemen die in strijd is met de taakstelling van de betrokkene en de doelstelling van de voorzieningen, alsmede activiteiten die strijdig zijn met wettelijke bepalingen, algemene afspraken binnen (onderdelen van) de UM, CAO-afspraken en afspraken zoals verwoord in de Bijlage “Gebruiksreglement MAASnet-faciliteiten UM”, behorende bij “GEBRUIKS- EN BEHEERSVOORWAARDEN MAASnet UM”.

Privetisering:
Privé gebruik van informatie of informatiesystemen dat zich beperkt tot algemeen geaccepteerde privé activiteiten binnen de geboden arbeidsvoorwaarden en voorzieningen. Hierover kunnen binnen de (deel)organisatie algemene nadere gedragsregels vastgesteld zijn. Een voorbeeld is het gebruik van telefoon of e-mail voor het maken van een afspraak onder kantoortijd.

DOEL VAN DIT DOCUMENT:

Deze code is bestemd voor ICT-functionarissen binnen de UM en geeft aan hoe deze functionarissen om dienen te gaan met informatie die zij uit hoofde van hun taakstelling verwerken en met de informatiesystemen die zij daartoe gebruiken.
Voor een aantal artikelen is een toelichting beschikbaar in Bijlage 1 van dit document, dit is aangegeven met (*).

ALGEMEEN:

Artikel 1

1.1 Deze integriteits- en gedragscode is van toepassing op ICT-functionarissen van de Universiteit Maastricht en is een verbijzondering van de CAO Nederlandse Universiteiten (1 jan. 2006 t/m 31-aug-2007), in het bijzonder van artikel 1.16 in die CAO, van de "GEBRUIKS- EN BEHEERSVOORWAARDEN MAASnet UM" en eventuele specifieke formele bepalingen binnen de (deel)organisatie waarvoor de betrokkene werkzaam is, zoals huisregels en regels omtrent privé-gebruik van informatiesystemen.

1.2 Het niet naleven van deze integriteits- en gedragscode kan leiden tot plichtsverzuim als bedoeld in de CAO Nederlandse Universiteiten (artikel 6.12 CAO NU). Door het CvB kan aan ICT-functionarissen die zich schuldig maken aan plichtsverzuim, een disciplinaire maatregel worden opgelegd.

1.3 Onder ICT-functionaris wordt voor de toepassing van deze code verstaan:

1. elke werknemer van de Universiteit Maastricht met een functie die behoort tot de functiefamilie ICT (UFO);
2. de directeur en staffunctionarissen van de (deel)organisatie waarvoor deze werknemer werkzaam is;
3. andere personen die op/voor de UM werkzaamheden verrichten op ICT-gebied onder verantwoordelijkheid van een organisatieonderdeel van de UM;
4. andere personen die op/voor de UM werkzaamheden verrichten ter ondersteuning van genoemde personen onder 1, 2 en 3 en daardoor kennis (kunnen) nemen van informatie met betrekking tot de werkzaamheden van deze personen.

INTEGRITEIT:

Artikel 2

Onverminderd het bepaalde in deze code is de ICT-functionaris verplicht tot geheimhouding van informatie die hem uit hoofde van zijn taakstelling ter kennis komt voor zover die verplichting hem uitdrukkelijk is opgelegd of die verplichting uit de aard van die informatie volgt (*). Deze verplichting geldt ook na beëindiging van het dienstverband.

Artikel 3

De in artikel 2 bedoelde verplichting bestaat niet tegenover hen, die vanwege hun taakstelling binnen de UM delen in de verantwoordelijkheid voor een goede uitoefening van de functie van de ICT-functionaris (*).

Artikel 4

Conform artikel 12, lid 1 van de Wet bescherming persoonsgegevens verwerkt de ICT-functionaris de persoonsgegevens waartoe hij toegang heeft, slechts in opdracht van het College van Bestuur of gemandateerde(n), behoudens afwijkende wettelijke verplichtingen.

Artikel 5

Conform artikel 12, lid 2 van de Wet bescherming persoonsgegevens is de ICT-functionaris verplicht tot geheimhouding van de persoonsgegevens waarvan hij uit hoofde van zijn functie kennis neemt, tenzij enig wettelijk voorschrift hem tot mededeling verplicht of uit zijn taak de noodzaak tot mededeling voortvloeit (*). Deze geheimhoudingsbepaling is een verplichting op grond van een wettelijk voorschrift als bedoeld in artikel 272 Wetboek van Strafrecht.

Artikel 6

De ICT-functionaris is zonder toestemming van de individuele medewerker of student niet bevoegd tot het lezen van documenten of e-mail of het meekijken met het gebruik van overige informatiesystemen van medewerkers en studenten tenzij onderzoek, gericht naar een incident of naar niet toegestaan gebruik daartoe noodzaakt (*).

Artikel 7

De ICT-functionaris zal gericht onderzoek naar een incident of niet toegestaan gebruik slechts uitvoeren indien er sprake is (geweest) van acute overlast door een of meerdere aangesloten werkstations of sprake is van (vermoeden van) ernstige bedreiging vanuit aangesloten werkstations of gebruikmakend van specifieke toegangscodes. Het onderzoek dient zich te beperken tot informatie of informatiesystemen die direct of indirect tot het beheersdomein van de ICT-functionaris behoren. De ICT-functionaris kan dan middels een actief onderzoek de status van het gebruik of het (netwerk)gedrag van betreffende stations of gebruikers vaststellen, daar een registratie van maken en zonodig maatregelen treffen om verder misbruik tegen te gaan, danwel verdere bedreigingen te beperken.
Indien er overigens sterke aanwijzingen bestaan dat er misbruik van de universitaire informatie of informatiesystemen wordt gemaakt of heeft plaatsgevonden, dan kan een nader onderzoek worden gedaan naar het gebruik van de universitaire informatie-voorzieningen door een individuele medewerker of student.
Dit nader onderzoek kan slechts worden verricht met toestemming van het CvB of van de daartoe gemandateerde directeur ICT Servicecentrum. Het onderzoek dient te worden uitgevoerd conform het bepaalde in artikel 5 van “GEBRUIKS- EN BEHEERS-VOORWAARDEN MAASnet UM”

Artikel 8

Indien bij steekproefsgewijze algemene controle op informatiestromen en/of het gebruik van informatiesystemen of bij onderzoek naar aanleiding van incidenten kennis genomen wordt van de inhoud van documenten of e-mail van medewerkers of studenten geldt geheimhoudingsverplichting niet ten opzichte van het College van Bestuur of de gemandateerde(n).

GEDRAG:

Artikel 9

De ICT-functionaris houdt zich in de praktijkuitoefening en in het bijzonder bij het gebruik van UM informatiesystemen en overige UM ICT-faciliteiten aan de bestaande wettelijke richtlijnen (zoals onder meer vastgesteld in de Wet Bescherming Persoonsgegevens, de Wet Computercriminaliteit, Wet op het auteursrecht) en de uitwerkingen daarvan voor de UM, almede aan de bepalingen in de "GEBRUIKS- EN BEHEERSVOORWAARDEN MAASnet UM". (*)

Artikel 10

De ICT-functionaris zal zich bij de uitoefening van zijn werkzaamheden onthouden van gedrag dat afbreuk doet aan het vertrouwen in de UM of het organisatieonderdeel waarvoor de functionaris werkzaam is namens de UM.

Artikel 11

De ICT-functionaris zal bij het gebruik van informatie de grootst mogelijke zorgvuldigheid betrachten. Dit houdt in dat de functionaris maatregelen neemt om te voorkomen dat derden informatie te zien krijgen, die niet voor hen bestemd is. Er wordt vanuit gegaan dat minimaal de volgende maatregelen genomen zijn om dit te bereiken:

- Er moet een zodanige toegangscontrole op de gebruikte systemen zijn, dat gegarandeerd kan worden dat alleen die gebruikers die daartoe bevoegd zijn, de systemen of data kunnen gebruiken, terwijl de toegang aan onbevoegde personen wordt ontzegd.
- Bovenstaande betekent dat de echtheid van de gebruikersidentiteit minimaal moet worden vastgesteld aan de hand van een gebruikersidentificatie en een wachtwoord. De gebruikte wachtwoorden dienen te voldoen aan de algemene richtlijnen voor goede wachtwoorden, zoals die door de UM zijn vastgesteld.
- Om meekijken door onbevoegden te voorkomen moeten beeldschermen zodanig opgesteld worden dat derden niet makkelijk mee kunnen lezen.
- Om misbruik tijdens (korte) afwezigheid te voorkomen moet de functionaris er voor zorgen dat tijdens die afwezigheid voor anderen geen gevoelige informatie op het systeem beschikbaar is, bij voorkeur door uit te loggen uit het systeem, of bijvoorbeeld door bij vertrek een screensaver met wachtwoord te activeren.

Artikel 12

De ICT-functionaris zal al hetgeen redelijkerwijs van hem verlangd mag worden, doen om de vertrouwelijkheid, integriteit en beschikbaarheid te waarborgen van de gegevens die aanwezig zijn op de voor hem toegankelijke UM-informatiesystemen.

Artikel 13

ICT-functionaris zal alle (vermeende) incidenten met betrekking tot informatie of informatiesystemen, die hem ter kennis komen direct melden aan zijn leidinggevende. De leidinggevende wordt geacht passende maatregelen te treffen ter voorkoming van herhaling van een dergelijk incident.

Artikel 14

De ICT-functionaris zal de aan hem in het kader van de werkzaamheden beschikbaar gestelde werkstations beheren conform de richtlijnen die voor betreffende werkstations zijn vastgesteld en geen aanpassingen aan de configuratie aanbrengen, anders dan noodzakelijk voor de eigen werkzaamheden. Indien aanpassingen noodzakelijk zijn die leiden tot een uitbreiding van de standaard communicatieprotocollen (netwerkprotocollen, peer-to-peer netwerken, etc.), dient hiervoor toestemming te worden gevraagd aan de functioneel beheerder van het werkstation of aan de leidinggevende.

Artikel 15

De ICT-functionaris zal alleen voor zover het noodzakelijk is voor de uitvoering van zijn werkzaamheden gebruik maken van de UM informatiesystemen en overige UM ICT-voorzieningen, daarbij inbegrepen alle voorzieningen voor externe toegang, zoals de inbel-, VPN- en Proxy-toegang.
Privé gebruik moet beperkt blijven tot het gebruik wat gerekend mag worden tot de “Privetisering” van de arbeidsvoorzieningen. In alle gevallen dient het gebruik in overeenstemming te zijn met het gestelde in artikels 9 en 14 van deze code.

Artikel 16

Elke ICT-functionaris krijgt specifieke bevoegdheden, benodigd voor het uitvoeren van werkzaamheden direct voortvloeiend uit de taakstelling van de ICT-functionaris. (*)
De ICT-functionaris mag deze bevoegdheden niet door anderen laten gebruiken.

Artikel 17

Het gebruik van de aan de ICT-functionaris toegekende specifieke bevoegdheden is werkgerelateerd. De bevoegdheden mogen niet voor andere doeleinden worden gebruikt dan werkzaamheden direct voortvloeiend uit de taakstelling van de ICT-functionaris.

Artikel 18

Bij wijzigingen in de werkzaamheden wordt de ICT-functionaris geacht aan de leidinggevende door te geven welke wijzigingen er in de bevoegdheden moeten plaats vinden. De leidinggevende dient de gewenste of noodzakelijke wijzigingen in de bevoegdheden door te geven aan de functioneel beheerder van het betreffende systeem(deel).

Artikel 19

Bij beëindiging van de arbeidsovereenkomst wordt de ICT-functionaris geacht aan de leidinggevende door te geven welke specifieke aanpassingen in bevoegdheden voor/door deze ICT-functionaris zijn aangebracht en dientengevolge bij zijn vertrek gewijzigd moeten worden. De leidinggevende dient de noodzakelijke wijzigingen in de bevoegdheden door te geven aan de functioneel beheerder van de betreffende (deel)systemen. Voorts is de leidinggevende verantwoordelijk voor het intrekken van overige algemene bevoegdheden van de vertrekkende ICT-functionaris (*). De ICT-functionaris wordt daarmee na vertrek gevrijwaard van verdere verantwoordelijkheid voor de vertrouwelijkheid, integriteit en beschikbaarheid van algemene en specifieke informatie en informatiesystemen.

Artikel 20

Deze code kan worden aangehaald als ‘Integriteits- en gedragscode ICT-functionarissen UM’.

Integriteits- en gedragscode ICT-functionarissen UM Bijlage I, toelichtingen

BIJLAGE I:

Korte toelichting Integriteits- en gedragscode ICT-functionarissen UM

Artikel 2

De ICT-functionaris wordt in staat geacht uit de aard van de informatie af te kunnen leiden of deze informatie een vertrouwelijk karakter heeft. Zo nodig kan de functionaris dit bij de leidinggevende toetsen.

Artikel 3

Het gaat hier dus om collega ICT-functionarissen die een directe betrokkenheid hebben bij het goed uitvoeren van een bepaalde taak. Het delen van informatie is noodzakelijk voor het goed uitoefenen van die taak.

Artikel 5

Dit is een nadere specificatie met betrekking tot geheimhouding van persoonsgegevens, omdat hierop specifieke wetgeving van toepassing is. Bij artikels 2 en 3 kan de informatie ook andersoortige kennis betreffen. Met de vermelding van het wetboek van strafrecht wordt een kader vastgelegd voor eventuele sancties.

Artikel 6

De noodzaak kan ondermeer voortvloeien uit (formele) klachten, wettelijke verplichtingen, uit steekproeven of uit beheersgegevens voortvloeiende (vermeende) bedreigingen.

Artikel 9

Het gaat hier om het algemene **eigen** gedrag van de ICT-functionaris. Ook de ICT-functionaris mag geen illegale software gebruiken etc.

Artikel 16

Het gaat dus om bevoegdheden die een normale gebruiker of een andere ICT-functionaris niet heeft.

Artikel 19

Het intrekken van algemene bevoegdheden zal doorgaans in een zogenaamde algemene Exit-procedure van de (deel)organisatie worden geregeld. Het blijft echter de verantwoordelijkheid van de leidinggevende.