Leidraad Integriteitcode

Datum: juni 2010

SurfIBO

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.

Inhoudsopgave

1. Inleiding

Tijdens de ontwikkeling van de leidraad voor de Acceptable Use Policy (AUP) voor eindgebruikers kwam al vrij snel de behoefte boven aan een integriteitcode specifiek gericht op beheerders/ ICT functionarissen. Deze specifieke groep gebruikers heeft vanuit haar functie vaak verregaande bevoegdheden binnen informatieverwerkende systemen. Door de tools die hen ter beschikking staan kunnen zij vaak op eenvoudige wijze privacygevoelige informatie verzamelen.

Geheimhoudingsplicht is zowel in de CAO van de Universiteiten als die van de HBO instellingen geregeld. Vandaar dat er een aantal instellingen zijn waar het regelen van een aparte integritietcode voor beheer als overbodig ervaren wordt. Het separaat aanbieden van een integriteitcode is echter een extra middel om de beheerder nadrukkelijk te wijzen op de specifieke verantwoordelijkheden die hij heeft waar het gaat om de omgang met vertrouwelijke informatie. Het zal dus zeker bijdragen aan een stukje bewustzijn bij de betreffende beheerder. Bovendien is bijvoorbeeld het intrekken van bevoegdheden bij vertrek/functiewijziging niet in de CAO geregeld. Middels artikel 16 en 17 in bijgevoegde code wordt een stukje verantwoordelijkheid voor het onderhouden van deze bevoegdheden bij de beheerder zelf gelegd.

2. Invoeren van een integriteitcode

Er zijn instellingen die ervoor kiezen om de integriteitcode door beheerders te laten ondertekenen. Vraag die dat altijd weer opwerpt is wat doe je dan als de betreffende medewerker weigert te ondertekenen? Hoeft deze zich dan ook niet aan de code te houden? Hoewel ondertekening een formelere status lijkt te geven aan de code is het juridisch gezien voor (interne) medewerkers niet noodzakelijk. De integriteitcode kan als werkinstructie gezien worden en is daarmee ook bindend voor de medewerkers die het betreft, voorwaarde is natuurlijk wel dat de betreffende medewerkers op de hoogte zijn gesteld van de inhoud van de code.

Bij inhuur van externe capacitiet verdient het de voorkeur om de code wel doorde inhuurkracht te laten ondertekenen.

3. Bronnen

Voor het opstellen van de Model Integriteitcode voor beheerders is gebruik gemaakt van de integriteitcodes die bij de Universiteit Maastricht, Universiteit van Tilburg en Hogeschool Windesheim in gebruik zijn.

Vanuit de integriteitcode wordt verwezen naar de lokale AUP en de CAO voor Universiteiten en HBO instellingen.

4. Model- Integriteitcode ICT functionarissen <organisatie>

Artikel 1

1. Deze integriteitcode is van toepassing op ICT-functionarissen van de **<organisatie>** en is een verbijzondering van artikel <E-1, leden 1 en 2, en artikel E-2 van de CAO voor het Hoger Beroepsonderwijs, 1.8 en 1.16 van de CAO Nederlandse Universiteiten>.
2. Onder ICT-functionaris wordt voor de toepassing van deze code verstaan:
   a. elke medewerker die in dienst is van <organisatie> en een functie vervult binnen <afdeling of functiefamilie ICT> van <organisatie>;
   b. de directeur van de <afdeling ICT> van <organisatie>;
   c. andere personen die werkzaamheden op ICT-gebied verrichten voor <organisatie>.

Artikel 2

Onverminderd het in de wet, de CAO voor **<het Hoger Beroepsonderwijs, Nederlandse Universiteiten>** en deze code bepaalde, is de ICT-functionaris verplicht tot geheimhouding van wat hem uit hoofde van zijn functie ter kennis komt voor zover die verplichting uit de aard der zaak volgt of hem uitdrukkelijk is opgelegd. Deze verplichting geldt ook na beëindiging van het dienstverband met **<organisatie>.**

Artikel 3

De in artikel 2 bedoelde verplichting bestaat niet in de situaties bedoeld in artikel **<vermeld hier het artikel uit de AUP waarin staat dat er controle op misbruik wordt uitgevoerd>** van **<organisatie>** (verder: het Reglement) tegenover hen, die delen in de verantwoordelijkheid voor een goede uitoefening van de functie van de ICT-functionaris.

Artikel 4

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

Artikel 5

Conform artikel 12 lid 2 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 dan wel uit zijn taak of uit bepalingen van het Reglement 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 van **<organisatie>** niet bevoegd tot het lezen van documenten of e-mail of het meekijken met het gebruik door medewerkers en studenten van overige informatiesystemen, waaronder internet, tenzij gericht onderzoek naar een incident of naar niet toegestaan gebruik van e-mail en/of informatiesystemen daartoe noodzaakt.

Artikel 7

De ICT-functionaris zal gericht onderzoek naar niet toegestaan gebruik van e-mail en/of informatiesystemen, conform **<vermeld betreffend artikel uit AUP>** van het Reglement, alleen na uitdrukkelijke en schriftelijke opdracht van het College van Bestuur of van de door het College van Bestuur gemandateerde(n) uitvoeren.

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 van **<organisatie>** geldt de geheimhoudingsverplichting van de ICT-functionaris als bedoeld in artikel **<E-2 lid 1 van de CAO voor het Hoger Beroepsonderwijs, 1.16 van de CAO Nederlandse Universiteiten>** niet ten opzichte van het College van Bestuur of de door het College van Bestuur gemandateerde(n).

Artikel 9

De ICT-functionaris houdt zich bij de uitoefening van zijn werkzaamheden en in het bijzonder bij het gebruik van informatiesystemen en overige ICT-faciliteiten van **<organisatie>** aan de bestaande wettelijke bepalingen en richtlijnen, zoals onder meer vastgesteld in de Wet Bescherming Persoonsgegevens, de Wet Computercriminaliteit en de Auteurswet en in de uitwerkingen daarvan voor **<organisatie>.**

Artikel 10

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

Artikel 11

De ICT-functionaris zal bij het gebruik van informatie de grootst mogelijke zorgvuldigheid betrachten. Dit houdt in ieder geval in dat de ICT-functionaris maatregelen neemt om te voorkomen dat derden informatie te zien krijgen, die niet voor hen bestemd is.

Artikel 12

De ICT-functionaris zal al wat 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 **<organisatie>**-informatiesystemen.

Artikel 13

De ICT-functionaris zal alle (vermeende) incidenten met betrekking tot onjuist gebruik en/of misbruik van informatie of informatiesystemen, die hem ter kennis komen direct melden aan zijn leidinggevende.

Artikel 14

De ICT-functionaris heeft specifieke bevoegdheden, benodigd voor het uitvoeren van werkzaamheden direct voortvloeiend uit zijn of haar functie en/of taken, waaronder in ieder geval taken die zijn vastgesteld in het Reglement.
De ICT-functionaris mag deze bevoegdheden niet door anderen laten gebruiken.

Artikel 15

Het gebruik van de aan de ICT-functionaris toegekende specifieke bevoegdheden is werkgerelateerd. De ICT-functionaris mag de bevoegdheden niet voor andere doeleinden gebruiken dan werkzaamheden direct voortvloeiend uit zijn of haar functie en/of taken.

Artikel 16

Bij wijzigingen in zijn of haar werkzaamheden wordt de ICT-functionaris, onverlet de verantwoordelijkheid ter zake van **<organisatie>,** geacht schriftelijk of per e-mail aan de leidinggevende door te geven welke wijzigingen er in de bevoegdheden moeten plaats vinden.

Artikel 17

Bij beëindiging van zijn of haar dienstverband met **<organisatie>** wordt de ICT-functionaris, onverlet de verantwoordelijkheid ter zake van **<organisatie>,** geacht schriftelijk of per e-mail 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.

Artikel 18

Het niet naleven van deze integriteits- en gedragscode kan vanwege plichtsverzuim leiden tot een door of namens het College van Bestuur te treffen disciplinaire maatregel als bedoeld in artikel **<P-4 lid 1 en lid 2 van de CAO voor het Hoger Beroepsonderwijs, 6.12 van de CAO Nederlandse Universiteiten>**.

Artikel 19

Deze code kan worden aangehaald als ‘Integriteitscode ICT-functionarissen **<organisatie>**’.

Artikel 20

Deze code treedt in werking op **<datum>.**

Bijlage bij Integriteitcode ICT-functionarissen <organisatie>

A. Uit de CAO voor het Hoger Beroepsonderwijs:

- Artikel E-1 Algemene verplichtingen

1. De werkgever en werknemer zijn verplicht zich als een goed werkgever en een goed werknemer te gedragen.

2. De werknemer is verplicht zijn functie naar beste vermogen te vervullen en zich daarbij te gedragen naar de aanwijzingen door of vanwege de werkgever gegeven.

- Artikel E-2 Geheimhouding

1. De werknemer is verplicht tot geheimhouding van hetgeen hem uit hoofde van zijn functie ter kennis komt, voor zover die verplichting uit de aard der zaak volgt of uitdrukkelijk schriftelijk is opgelegd. Deze verplichting geldt ook na beëindiging van de arbeidsovereenkomst.

2. Onverminderd wettelijke bepalingen is de werkgever jegens derden verplicht tot geheimhouding van persoonlijke gegevens van de werknemer, tenzij de werknemer tot het verstrekken van op zijn persoon betrekking hebbende gegevens schriftelijk toestemming geeft.

- Artikel P-4 Disciplinaire maatregelen

1. De werknemer die niet doet dan wel nalaat wat een goed werknemer in gelijke omstandigheden behoort te doen of na te laten kan door de werkgever een disciplinaire maatregel worden opgelegd.

2. De werkgever kan ten aanzien van de werknemer de volgende disciplinaire maatregelen treffen:

a schriftelijke berisping;

b overplaatsing;

c schorsing;

d ontslag.

A. Uit de CAO Nederlandse Universiteiten:

- Artikel 1.8 Algemeen

2. De werknemer is gehouden zijn functie naar zijn beste vermogen uit te oefenen, zich te gedragen als een goed werknemer en te handelen naar de aanwijzingen door of vanwege de werkgever gegeven.

- Artikel 1.16 Geheimhouding

1. De werknemer is verplicht tot geheimhouding van hetgeen hem uit hoofde van zijn functie ter kennis komt, voor zover die verplichting uit de aard der zaak volgt of hem uitdrukkelijk is opgelegd. Deze verplichting geldt ook na beëindiging van het dienstverband.

2. De in lid 1 bedoelde verplichting bestaat niet tegenover hen, die delen in de verantwoordelijkheid voor een goede uitoefening van zijn functie door de werknemer, noch tegenover hen, wier medewerking bij die uitoefening noodzakelijk is te achten, indien en voor zover deze zelf tot geheimhouding verplicht zijn of zich daartoe verplichten. Het in de vorige zin gestelde geldt met inachtneming van wettelijke bepalingen inzake het beroepsgeheim.

Artikel 6.10 Algemeen

Indien een werkgever aan een werknemer van een openbare universiteit een disciplinaire maatregel oplegt, is het bepaalde in deze paragraaf van toepassing.

- Artikel 6.12 Disciplinaire maatregelen

1. De werkgever kan aan de werknemer die zich aan plichtsverzuim schuldig maakt een disciplinaire maatregel opleggen welke in verhouding staat tot het plichtsverzuim.

2. Plichtsverzuim omvat zowel het overtreden van enig voorschrift als het doen of nalaten van iets, wat een goed werknemer in gelijke omstandigheden behoort na te laten of te doen.

3. De werkgever kan met betrekking tot het opleggen van een disciplinaire maatregel nadere regels vaststellen.

B. Uit de Wet bescherming persoonsgegevens:

- Artikel 12
1. Een ieder die handelt onder het gezag van de verantwoordelijke of van de bewerker, alsmede de bewerker zelf, voor zover deze toegang hebben tot persoonsgegevens, verwerkt deze slechts in opdracht van de verantwoordelijke, behoudens afwijkende wettelijke verplichtingen.

2. De personen, bedoeld in het eerste lid, voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennis nemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit. Artikel 272, tweede lid, van het Wetboek van Strafrecht is niet van toepassing.

C. Uit het Wetboek van Strafrecht:

- Artikel 272

1. Hij die enig geheim waarvan hij weet of redelijkerwijs moet vermoeden dat hij uit hoofde van ambt, beroep of wettelijk voorschrift dan wel van vroeger ambt of beroep verplicht is het te bewaren, opzettelijk schendt, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie.

2. Indien dit misdrijf tegen een bepaald persoon gepleegd is, wordt het slechts vervolgd op diens klacht.

D. Uit de AUP:

Artikel vermelden dat aangehaald wordt in artikel 7 van deze integriteitcode.