

Geachte lezer,

Volgens een definitie is veiligheid de mate van afwezigheid van potentiële oorzaken van een gevaarlijke situatie of de mate van aanwezigheid van beschermende maatregelen tegen deze potentiële oorzaken. Veiligheid is ook een relatief begrip, aangezien niets onder alle omstandigheden volledig zonder gevaar is. Sommigen zien de oplossing van het gevaar als enkel een kwestie van organisatorische en technische maatregelen. Het begrip veiligheid bestaat echter zowel rationeel als denkbeeldig. Rationeel kunnen er allerlei berekeningen worden toegepast op een situatie om te bepalen of deze veilig is. Daarnaast is er nog denkbeeldige veiligheid. Iemand kan zich veilig voelen maar het rationeel gezien niet zijn en andersom. Dit wordt ook wel schijnveiligheid (resp. schijnonveiligheid) genoemd.

Het project Integrale Veiligheid in het Hoger Onderwijs, fase 2 onderkent het bovenstaande en legt juist daarom het accent op de menselijke component. Het versterken van de individuele veiligheidsbeleving gepaard met een hoger veiligheidsbewustzijn (awareness) kunnen het gedrag op het gebied van veiligheid in aanzienlijke mate in positieve zin veranderen. Deze uitkomst beïnvloedt vervolgens de keuzes die gemaakt worden voor effectieve inzet van allerlei instrumenten. Risicomanagement is daarnaast een rode draad in de opzet van integrale veiligheid. Kostenbesparing moet logischerwijs een gevolg zijn van deze gecombineerde aanpak.

Deze uitgangspunten vormen de basis voor de werkzaamheden in de werkgroepen. Het (hoger) onderwijs kent op het gebied van integrale veiligheid nog een bijzondere uitdaging. Het open en vriendelijke karakter van onderwijsinstellingen staat soms op gespannen voet met de mate waarin veiligheid moet zijn geregeld. Binnen de projectgroepen van governance, bewustwording, informatiebeveiliging, privacy, kennisveiligheid en integriteit en internationalisering heb ik in de afgelopen maanden met bewondering gezien hoe de projecttrekkers en de projectleden hun soms uiteenlopende onderwerpen binnen het domein integrale veiligheid tot een samenhangend geheel weten te smeden. Waardevolle instrumenten die zowel de bestuurder als de student straks goed kunnen gebruiken. Vanuit de opdrachtgever OCW maar ook de VSNU en de Vereniging Hogescholen worden de ontwikkelingen nauwlettend gevolgd. In volgende nieuwsbrieven geven zij hun kijk op de ontwikkelingen in deze fase van het project Veilig Hoger Onderwijs.

Deze nieuwsbrief, die ik met plezier bij u introduceer, geeft u inzicht in de tussenstand van de resultaten bij de verschillende projectgroepen. Ik wens u veel leesplezier en hoop u op ons afsluitende symposium te mogen begroeten. De uitnodiging voor deze bijeenkomst gaat u binnenkort toe. Reserveer 22 mei alvast in uw agenda. De locatie is de Oude Lutherse Kerk in Amsterdam.

Met vriendelijk groet,
Ron Massink
Voorzitter

Governance en het wettelijke speelveld

Governance kan worden gerelateerd aan consistent management, samenhangend beleid, processen en beslissingsrechten voor een bepaalde bevoegdheid. Dit alles vindt in het hoger onderwijs plaats in een speelveld met een kader van wet en regelgeving specifiek van toepassing voor het hoger onderwijs. Er is in dit speelveld ook een specifiek kader als het gaat om veiligheid. Dit kader is afhankelijk van specifieke onderwijs- en onderzoeksactiviteiten. Inzicht in dit kader is noodzakelijk om uw governance op orde te hebben. Het deelproject Governance helpt u bij het verkrijgen van dit inzicht. Uw bijdrage is daarbij echter ook noodzakelijk. [Lees meer.](#)

Thema's

- Governance
- Social Media
- Integriteit
- Privacy
- Informatieveiligheid
- Internationaal
- Huiselijk geweld
- Goed bestuur



Social media in het hoger onderwijs



De hulpmiddelen in het onderwijs zijn in de periode van 1950 tot heden sterk ontwikkeld. Van schoolboek, schoolbord en krijtjes naar het gebruik van Ipads, smartphones en blackboard. De ontwikkelingen ten aanzien van het gebruik van social media zijn in de laatste 5 jaren dermate ingrijpend dat ook van docenten in het hoger onderwijs verwacht kan worden dat zij geconfronteerd zullen worden met de gevolgen hiervan. Studenten maken bijna zonder uitzondering gebruik van facebook en twitter.

Vanwege de jongste ontwikkelingen (google glass, horloges - pebbles - die gelinkt zijn aan smartphones, camerapennen) wordt het als noodzakelijk ervaren dat instellingen voor hoger onderwijs zich oriënteren op het gebruik van nieuwe media in het onderwijs. Bijvoorbeeld wat te doen bij de afname van tentamens? Deze ontwikkelingen vragen om de opstelling van een gedragscode ten aanzien van social media. [Lees meer.](#)

Dag van de integriteit 2013

Het jaarlijkse evenement, georganiseerd door Bureau Integriteitsbevordering Openbare Sector (BIOS), draaide ditmaal om integer leiderschap en bestuur. Veel sprekers benadrukken dat integriteit een kwestie is van houding, gedrag, gezond verstand en het elkaar leren aanspreken. Bestuurders moeten daarin een voorbeeldfunctie hebben en de integriteit moet in alle lagen van de organisatie onderwerp van gesprek zijn.



Voor Doekle Terpstra (InHolland) ligt de bal nu bij bestuurders zelf. Meer regels en codes zijn niet nodig: 'Zoals we ook concludeerden in het rapport-Halsema moet het semipublieke domein nu zelf een dialoog voeren over integriteit en haar publieke opdracht. In het debat over moreel leiderschap lag de nadruk op elkaar aanspreken, eerlijk zijn en gezond verstand gebruiken. 'Integriteit zit in de mensen zelf, dat kun je niet met regeltjes vastleggen' stelde Thom de Graaf, 'Integriteit betekent: als je twijfelt doe het niet, wil je het toch doen, ga dan voor de spiegel staan, spreek het uit en stel je voor dat je het tegen een ochtendkrant vertelt.' [Lees meer](#)

Europese privacy verordening (EPV) op komst: hoger onderwijs bereidt zich samen voor



In Brussel wordt de laatste tijd hard gewerkt aan de uitwerking van de nieuwe privacy verordening die de huidige privacy wetgeving gaat vervangen. De Europese Commissie stelt grondige hervorming van gegevensbeschermings-regels voor: meer controle over de eigen persoonsgegevens, minder kosten voor bedrijven.

Enkele elementen uit de concept verordening: Elk bedrijf/organisatie is momenteel verplicht om alle maatregelen inzake gegevensbescherming aan de toezichthouders te melden. Straks moeten verwerkers van persoonsgegevens meer verantwoording en rekenschap afleggen. Ernstige gegevenslekken moeten zo snel mogelijk (zo mogelijk binnen 24 uur) aan de nationale toezicht-houder worden gemeld, dit is een taak voor de

Functionaris Gegevensbescherming. Mensen zullen gemakkelijker toegang krijgen tot hun eigen gegevens en hun persoons-gegevens gemakkelijker van de ene dienstverstrekker naar de andere kunnen overdragen (recht op gegevensover-draagbaarheid). Het CBP zal meer bevoegdheden krijgen om de EU-regels in Nederland te doen eerbiedigen, onder meer om boetes op te leggen aan bedrijven/organisaties die die regels overtreden. Die boetes kunnen oplopen tot 1 miljoen euro of tot 5% van de totale jaarlijkse omzet van een bedrijf/organisatie. Daarmee is voor (onderwijs)instellingen sprake van een materieel risico, waar accountants naar moet kijken. [Lees meer.](#)

15 Januari 2014: 'In de Steigers'

Congres iBestuur: Integratie aanpak (informatie)veiligheid in het hoger onderwijs

De iOverheid staat inmiddels goed in de steigers. Op 15 januari 2014 buigden 900 deelnemers zich over de voortgang van allerlei ict-bouwprojecten van overheid en semi-overheid tijdens het iBestuur Congres 2014. Op dit congres konden de deelnemers ook kennis maken met de manier waarop de ketenpartners in het hoger onderwijs zorg dragen voor een integrale aanpak van informatieveiligheid in het hoger onderwijs, in workshops en tijdens het CIO Café.



Paul Rullmann, voorzitter Wetenschappelijk Technische Raad van SURF, oud-bestuurder TUDelft, en Doekle Terpstra, voorzitter College van Bestuur Inholland, vertelden hun verhaal over risicomanagement in het hoger onderwijs aan de hand van recente ontwikkelingen en geleerde lessen over informatieveiligheid, privacy-bescherming en cybersecurity. Welke risico's hebben zij gezien, waardoor werden die veroorzaakt, met welke gevolgen zijn ze geconfronteerd en hoe hebben ze die risico's beheersbaar gemaakt? Ze pleiten voor een integrale veiligheidsinfrastructuur, zoals deze in het project Integraal Veilig Hoger Onderwijs wordt ontwikkeld voor hogescholen en universiteiten. [Lees meer.](#)

Handreiking voor signalering en begeleiding veiligheids- en leefstijlrisico's in het hoger onderwijs



De Hogeschool Rotterdam heeft als eerste het initiatief genomen veiligheids- en leefstijlrisico's te agenderen binnen de eigen instelling om voor signalering, inschatting en aanpak van veiligheidsrisico's in het hbo een handreiking te ontwikkelen. Deze handreiking is in belangrijke mate gebaseerd op de ervaringen die zijn opgedaan in de Hogeschool Rotterdam waar een pilot is uitgevoerd.

Veel hogescholen zien hun studentenpopulatie de laatste jaren sterk veranderen naar een pluriforme doelgroep met een grote diversiteit en uiteenlopende culturele waarden. Dat stelt docenten en ander personeel voor ingewikkelder handelingsvragen op het gebied van gedrag en omgangsvormen. Maar ook neemt hiermee de complexiteit van de problematiek bij individuele studenten toe. En die problematiek komt ook de school binnen. [Lees meer.](#)

Veiligheid ook in het buitenland

Uw studenten en medewerkers kunnen ook in het buitenland geconfronteerd worden met onveiligheid. Dit blijkt wel uit een verslag van een aantal studenten van de TU Delft (<https://intranet.tudelft.nl/nl/citg/nieuws/artikel/detail/overvallen-in-mozambique> en <http://delta.tudelft.nl/artikel/avontuur-in-afrika/26215>).

Hier kunt u lezen dat het noodzakelijk is veilig internationaliseren op te nemen in uw integrale veiligheidsmaatregelen. Hieruit blijkt tevens dat er op het gebied van veiligheid voor studie- en werk gerelateerde activiteiten in het buitenland een aantal zaken breed geregeld zouden kunnen worden zoals bijvoorbeeld een gezamenlijke verzekering, een gezamenlijke incidenten registratie- en crisismanagement systeem.



Het project Veilig Internationaliseren wil dat voor bovengenoemde en andere risico's voor studenten en medewerkers (externe en interne mobiliteit) de juiste pro- en reactieve maatregelen op efficiënte en effectieve wijze worden ontwikkeld en uitgevoerd. Om dit te bereiken zijn de afgelopen tijd de veel voorkomende risico's op het gebied van interne en externe mobiliteit met bijbehorende maatregelen in kaart gebracht. [Lees meer.](#)

Meldcode Huiselijk geweld en kindermishandeling



Met ingang van 1 juli 2013 zijn beroepskrachten binnen onderwijsinstellingen, ook in het hoger onderwijs, verplicht een meldcode te gebruiken bij signalen van huiselijk geweld of kindermishandeling.

Elke onderwijsinstelling maakt de meldcode specifiek voor de eigen praktijk. Bijvoorbeeld door te benoemen wie de stappen moet doorlopen. Zo kan een instelling afspreken dat de melder de signalen bespreekt met de vertrouwenspersoon. Ook kan het nodig zijn in de meldcode extra aandacht te besteden aan signalering en handelwijze bij specifieke vormen van geweld. Een model voor een meldcode is te vinden op Rijksoverheid.nl. [Lees meer.](#)

Code goed bestuur hogescholen

Op 3 oktober hebben de hogescholen ingestemd met de Code goed bestuur die voortbouwt op de tot dan geldende Branchecode governance hbo. In de nieuwe code zijn de aanbevelingen verwerkt van de commissie Van Montfort, die in opdracht van het bestuur van de Vereniging Hogescholen de governancecode heeft geëvalueerd. Gebleven zijn de verplichting tot het hebben van een integriteitcode, een klokkenluiderregeling en een regeling ongewenst gedrag als onderdelen van een risicomanagement systeem. [Lees meer.](#)





Governance

Governance kan worden gerelateerd aan consistent management, samenhangend beleid, processen en beslissingsrechten voor een bepaalde bevoegdheid. Dit alles vindt in het hoger onderwijs plaats in een speelveld met een kader van wet en regelgeving specifiek van toepassing voor het hoger onderwijs. Er is in dit speelveld ook een specifiek kader als het gaat om veiligheid. Dit kader is afhankelijk van specifieke onderwijs- en onderzoeksactiviteiten. Inzicht in dit kader is noodzakelijk om uw governance op orde te hebben. Het deelproject Governance helpt u bij het verkrijgen van dit inzicht. Uw bijdrage is daarbij echter ook noodzakelijk.

Het deelproject Governance heeft een eerste verkenning gemaakt van het juridisch kader waar HO instellingen mee te maken hebben. Dit zal begin 2014 aan de instellingen worden gezonden voor feedback en aanvullingen. Veel wet- en regelgeving zal gelden voor alle instellingen, daarnaast realiseren wij ons terdege dat afhankelijk van de onderwijs- en onderzoeksactiviteiten bijzondere wetgeving van toepassing kan zijn. Voor het verkrijgen van een zo compleet mogelijk kader is de feedback van de instellingen dus van groot belang. Hiermee doen we dus alvast een beroep op uw medewerking. Het juridisch kader zal naast wet- en regelgeving op het gebied van veiligheid ook andere regelgeving benoemen die voor de instellingen in het kader van governance van belang kan zijn. In de uiteindelijke uitwerking van de toetsingsinstrumenten wordt conform onze opdracht alleen wet- en regelgeving meegenomen relevant voor veiligheid.

Voor het toetsingskader maakt de projectgroep Governance gebruik van de High Level Structure voor management systemen, inmiddels is deze omgezet naar een eerste versie van het toetsingskader. Door gebruik te maken van de High Level Structure sluit de projectgroep aan bij de ontwikkelingen inzake normen voor management systemen. De projectgroep onderzoekt op dit moment hoe het toetsingskader, handboek veiligheid en benchmark model voor veiligheid zo pragmatisch mogelijk kunnen worden geïntegreerd in elkaar.



Netwerk Universitaire Vertrouwenspersonen voorgelicht over social media in het hoger onderwijs

Op 14 november 2013 verzorgde Alf Moens, security officer van SURF, een presentatie over het gebruik van social media in het hoger onderwijs tijdens een overleg van het Netwerk Universitaire Vertrouwenspersonen. De presentatie was een voortvloeisel uit de samenwerking binnen het project Integriteit, Spionage, Informatieveiligheid en Cybercrime (ISIC).

Alf Moens schetste de ontwikkeling van hulpmiddelen in het onderwijs in de periode van 1950 tot heden. Van schoolboek, schoolbord en krijtjes naar het gebruik van Ipads, smartphones en blackboard. De ontwikkelingen ten aanzien van het gebruik van social media zijn in de laatste 5 jaren dermate ingrijpend dat ook van docenten in het hoger onderwijs verwacht kan worden dat zij geconfronteerd zullen worden met de gevolgen hiervan. Studenten maken bijna zonder uitzondering gebruik van facebook en twitter.

Betekent dat dan dat docenten en begeleiders eveneens gebruik moeten maken van deze media? En welk gevolg heeft het gebruik van social media ten aanzien van de werktijden? Waar men vroeger van half negen tot zes werkte, is er nu 24 uur per dag communicatie via twitter en facebook. Dat docenten en begeleiders geen (facebook-) "vrienden" moeten worden met studenten stond voor de vertrouwenspersonen als een paal boven water.

Vanwege de jongste ontwikkelingen (google glass, horloges - pebbles - die gelinkt zijn aan smartphones, camera-pennen) wordt het als noodzakelijk ervaren dat instellingen voor hoger onderwijs zich oriënteren op het gebruik van nieuwe media in het onderwijs. Bijvoorbeeld wat te doen bij de afname van tentamens? Smartphones en horloges bij binnenkomst in de onderwijsruimte innemen? En hoe gaan wij om met opnames van colleges, met verspreiding van werkgroepoverleg via youtube? Deze ontwikkelingen vragen om de opstelling van een gedragscode ten aanzien van social media. Enkele vertrouwenspersonen bepleitten het ondertekenen van een social media policy door alle studenten. Dat er afspraken zullen moeten worden gemaakt, lijkt onvermijdelijk.

Netwerk Universitaire Vertrouwenspersonen

Het Netwerk Universitaire Vertrouwenspersonen (NUV) is een samenwerkingsverband van de vertrouwenspersonen die werkzaam zijn aan Nederlandse universiteiten. Het NUV komt drie keer per jaar bijeen. Het netwerk is bedoeld ter uitwisseling van ervaringen van (dikwijls) solistisch opererende vertrouwenspersonen. Daar vertrouwenspersonen werken onder ambtsgeheim is uitwisseling van ervaringen binnen de eigen instelling niet altijd mogelijk. Onder vakgenoten kan uitwisseling wel plaats vinden. Tijdens vergaderingen wordt onder meer gesproken over klachtenprocedures, integriteitskwesaties, de gevolgen van het gebruik van social media door docenten en studenten, professionalisering van de vertrouwenspersoon, de uitvoering van de klokkenluidersregeling door de vertrouwenspersoon, de certificering van de vertrouwenspersoon, trends in het werk van de vertrouwenspersonen, enz. Een aantal vertrouwenspersonen werkt voor studenten, een aantal andere vertrouwenspersonen werkt voor personeel. Sommigen werken zowel voor studenten, als voor personeelsleden.



Dag van de Integriteit 2013 met bijdragen vanuit het hoger onderwijs!

Donderdag 14 november vond de vijfde Dag van de Integriteit plaats in Utrecht. Het jaarlijkse evenement, georganiseerd door Bureau Integriteitsbevordering Openbare Sector (BIOS), draaide ditmaal om integer leiderschap en bestuur. De Dag van de Integriteit is een jaarlijks initiatief van BIOS om de onderlinge kennisdeling over de integere overheid te stimuleren. Ditmaal heeft het accent gelegen op goed leiderschap en bestuur. Veel sprekers benadrukken dat integriteit een kwestie is van houding, gedrag, gezond verstand en het elkaar leren aanspreken. Bestuurders moeten daarin een voorbeeldfunctie hebben en de integriteit moet in alle lagen van de organisatie onderwerp van gesprek zijn. InHolland-bestuurder Doekle Terpstra sprak openhartig over zijn visie op leiderschap en integriteit. Vanuit het hoger onderwijs nam Thom de Graaf, voorzitter van de Vereniging Hogescholen (VH), actief deel aan het debat. (verslag http://www.dagvandeintegriteit.nl/editie_2013/verslag.shtml)

Integer leiderschap

Wat is er nodig om integriteit te bevorderen? Voor Doekle Terpstra (InHolland) ligt de bal nu bij bestuurders zelf. Meer regels en codes zijn niet nodig: 'Zoals we ook concludeerden in het rapport-Halsema moet het semipublieke domein nu zelf een dialoog voeren over integriteit en haar publieke opdracht.' Voor de meeste betrokkenen is dat een 'verduveld lastig gesprek', weet Terpstra: 'Veel bestuurders en toezichthouders zijn hierin niet geoefend. Het vraagt vaardigheid en kwetsbaarheid van bestuurders om dat lastige gesprek te voeren.' Het gesprek over integer handelen is meer dan een praatje voor de vaak. Het gaat over de maatschappelijke opdracht en over verantwoordelijkheden, ook in het hoger onderwijs!

(rapport: <http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2013/09/11/een-lastig-gesprek-advies-commissie-behoorlijk-bestuur/advies-commissie-behoorlijk-bestuur.pdf>)

'Integriteit betekent: als je twijfelt doe het niet'

In het debat over moreel leiderschap lag de nadruk op elkaar aanspreken, eerlijk zijn en gezond verstand gebruiken. 'Integriteit zit in de mensen zelf, dat kun je niet met regeltjes vastleggen' stelde Thom de Graaf, 'Integriteit betekent: als je twijfelt doe het niet, wil je het toch doen, ga dan voor de spiegel staan, spreek het uit en stel je voor dat je het tegen een ochtendkrant vertelt.'

In de nieuwe branchecode vraagt de Vereniging Hogescholen de leden zich gezamenlijk aan de gedragscode te houden. De leden confronteren elkaar met signalen bij hogescholen. Bestuurders, toezichthouders en de VH gaan het gesprek met elkaar aan. Het gaat daarbij om voorbeeldgedrag en om een integere cultuur. Als voorzitter biedt hij een luisterend oor voor de leden/bestuurders (Ik zit ergens mee, nl. hiermee ...), bij signalen neemt hij zijn verantwoordelijkheid.

Jaarboek Integriteit 2013

Minister Stef Blok (Wonen en Rijksdienst) nam het eerste exemplaar van het Jaarboek Integriteit 2013 in ontvangst. Dit jaar ligt het accent op bestuurlijke integriteit.

De deelnemers aan de Dag van de Integriteit kregen in het Mediaplaza een veelzijdig, inhoudelijk programma voorgeschoteld. Hoogleraar Muel Kaptein onderzocht de rol van de integriteitfunctionaris.

(Jaarboek Integriteit 2013: http://www.integriteitoverheid.nl/fileadmin/BIOS/data/Publicaties/Downloads/1306540_BIOS_Jaarboek_2013_web.pdf)

“Kan dat zo wel?”...

Een vraag waarvoor elke professional zich wel eens geplaatst ziet, zo ook in het hoger onderwijs.

BIOS ondersteunt hogescholen en universiteiten in het omgaan met integriteitvraagstukken door in het project Integraal Veilig Hoger Onderwijs (www.integraalveilig-ho.nl) samen met betrokkenen bij het hoger onderwijs op te trekken.

Behoeft aan moreel kompas

Integriteit vormt de hoeksteen van professioneel handelen. Het is een kernwaarde van en drijfveer voor professionals, in alle sectoren van de samenleving. Mensen koersen op hun moreel kompas om vanuit een intrinsieke motivatie de goede dingen te doen en de dingen goed te doen. Naast deze interne factoren spelen bij de uitvoering van werkzaamheden ook externe prikkels een rol. Soms ontstaat een onbalans tussen intrinsieke en extrinsieke motivatie waardoor het moreel kompas van slag kan raken. De morele balans tussen wat ‘wel’ en niet (meer) door de beugel kan, raakt ontregeld. Dan is er mogelijk sprake van integriteitschending. Op verschillende plekken duiken kwesties op die duiden op gebrek aan integer handelen, recent ook rondom voorheen betrouwbaar geachte sectoren in de samenleving. Incidenten bij banken, woningcorporaties, ziekenhuizen, onderwijsinstellingen en wetenschap leiden tot maatschappelijke verontwaardiging en geschonden vertrouwen.

Voorkomen is beter dan genezen

Beschadigd vertrouwen laat zich niet altijd vanzelfsprekend herstellen en vraagt vaak veel tijd en energie. In onze samenleving speelt vertrouwen een belangrijke rol, zo ook in het hoger onderwijs en onderzoek. Het bepaalt in hoge mate hoe we tegen elkaar aan kijken en hoe we met elkaar omgaan.

De remedie voor herstellen van vertrouwen is voorkómen. Tijd om stil te staan bij waar het eigenlijk om gaat bij integriteit in het hoger onderwijs. Het hoog houden en garanderen van kwalitatief goed en betrouwbaar onderwijs en onderzoek is een verantwoordelijkheid die betrokkenen, studenten, medewerkers en bestuurders alleen samen kunnen waarmaken. Aandacht voor integriteit, professioneel en wetenschappelijk, is daarbij cruciaal.

Samen optrekken

Reden temeer om samen met het hoger onderwijs na te gaan hoe de sector de vinger aan de pols houdt en werk maakt van integer handelen op alle niveaus, van studenten, medewerkers en onderzoekers tot bestuur en toezichthouders. In het project Integraal Veilig Hoger Onderwijs ondersteunt BIOS vanuit een integrale kijk op veiligheid en integriteit het hoger onderwijs bij het ontwikkelen van instrumenten om risico's ten aanzien van integriteit in kaart te brengen en te hanteren.



Europese Privacy Verordening (EPV) op komst: hoger onderwijs bereidt zich samen voor!

In het project Integraal Veilig Hoger Onderwijs wordt door SURF en ISIC hard gewerkt om goed voorbereid te zijn zodra de nieuwe EPV van kracht wordt. De EPV wordt waarschijnlijk van kracht in de loop van 2014, uiterlijk 2015. Er komen workshops, handreikingen, een model plan van aanpak, voorbeelden van Privacy Impact Assessments. In het project Integraal Veilig Hoger Onderwijs worden koepels, hogescholen en universiteiten uitgenodigd om met overheid en ketenpartners gezamenlijk op te trekken.

Waar gaat het om?

In Brussel wordt de laatste tijd hard gewerkt aan de uitwerking van de nieuwe privacy verordening die de huidige privacy wetgeving gaat vervangen. De Europese Commissie stelt grondige hervorming van gegevensbeschermingsregels voor: meer controle over de eigen persoonsgegevens, minder kosten voor bedrijven. De voorstellen van de Europese Commissie zijn een toekomstgerichte actualisering van de in de gegevensbeschermingsrichtlijn van 1995 vervatte beginselen om de privacyrechten te waarborgen. Het recht op bescherming van persoonsgegevens wordt uitdrukkelijk erkend in artikel 8 van het Handvest van de grondrechten van de Europese Unie en in het Verdrag van Lissabon. De rechtsgrondslag voor regelgeving inzake gegevensbescherming ten aanzien van alle activiteiten die binnen het toepassingsgebied van het EU-recht vallen, is artikel 16 van het Verdrag betreffende de werking van de Europese Unie. Het Europees Parlement buigt zich over meer dan 4000 amendementen.

Brussel, 25 januari 2012 – De Europese Commissie heeft vandaag een grondige hervorming van de EU-gegevensbeschermingsregels van 1995 voorgesteld om de privacy online beter te waarborgen en de digitale economie in Europa te stimuleren. De manier waarop gegevens worden verzameld, geraadpleegd en gebruikt, is door de technologische vooruitgang en de globalisering ingrijpend veranderd. Tevens hebben de 27 EU-lidstaten de regels van 1995 verschillend omgezet, wat tot verschillen in toepassing en handhaving heeft geleid. Een geïntegreerde wetgeving moet een einde maken aan de huidige fragmentatie en aan dure administratieve formaliteiten, waardoor bedrijven circa 2,3 miljard euro per jaar kunnen besparen. Met het initiatief moet het consumentenvertrouwen in onlinediensten worden aangewakkerd, wat de groei, werkgelegenheid en innovatie in Europa de noodzakelijke impulsen kan geven. Europese Commissie Persbericht 25 januari 2012; http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

Enkele elementen uit de concept verordening:

- Eén stel regels inzake gegevensbescherming, geldend in de gehele EU.
- Elk bedrijf/organisatie is momenteel verplicht om alle maatregelen inzake gegevensbescherming aan de toezichthouders te melden. Straks moeten verwerkers van persoonsgegevens meer verantwoording en rekening afleggen.
- Ernstige gegevenslekken moeten zo snel mogelijk (zo mogelijk binnen 24 uur) aan de nationale toezichthouder worden gemeld, taak voor de Functionaris Gegevensbescherming.
- Organisaties krijgen te maken met slechts één nationale gegevensbeschermingsautoriteit, in de EU-lidstaat waar zij hun belangrijkste vestiging hebben: in Nederland is dat het College Bescherming Persoonsgegevens.
- Mensen zullen gemakkelijker toegang krijgen tot hun eigen gegevens en hun persoonsgegevens gemakkelijker van de ene dienstverstrekker naar de andere kunnen overdragen (recht op gegevensoverdraagbaarheid).
- Een 'recht om te worden vergeten' moet mensen in staat stellen om privacy-risico's op internet beter te beheren, d.w.z. hun gegevens te wissen als er geen gegronde redenen zijn om ze te bewaren.
- Het CBP zal meer bevoegdheden krijgen om de EU-regels in Nederland te doen eerbiedigen, onder meer om boetes op te leggen aan bedrijven/organisaties die die regels overtreden. Die boetes kunnen oplopen tot 1 miljoen euro of tot 5% van de totale jaarlijkse omzet van een bedrijf/organisatie. Daarmee is voor (onderwijs) instellingen sprake van een materieel risico, waar accountants naar moet kijken.
- De rechten van het kind (tot 18 jaar) worden extra beschermd.
- Er is sprake verplichting tot 'privacy by design' (aan alle privacy-vereisten voldoen bij het ontwerp) en 'privacy by default' (alleen bewaren wat strikt noodzakelijk is), profiling mag niet.
- Elke bestuurder is verantwoordelijk voor naleving van het privacybeleid.

Welke steun is reeds voorhanden?

SURF heeft met betrokkenheid van deelproject Integriteit, Spionage, Informatieveiligheid, Cybercrime een initiatiefgroep 'EPV en impact voor hoger onderwijs' opgericht waarbinnen de voorbereidingen om te komen tot één sectorale aanpak om de impact van de EPV te vertalen naar het hoger onderwijs en de voorbereidingen ter hand te nemen. Via deze nieuwsbrief houden we instellingen op de hoogte van de voortgang in de ontwikkelingen.



15 januari 2014: 'In de steigers'

Congres iBestuur: Integrale aanpak (informatie) veiligheid in het hoger onderwijs

De iOverheid staat inmiddels goed in de steigers. Op 15 januari 2014 buigden zich 900 deelnemers over de voortgang van allerlei ict-bouwprojecten van overheid en semi-overheid tijdens het iBestuur Congres 2014. Op dit congres konden de deelnemers ook kennis maken met de manier waarop de ketenpartners in het hoger onderwijs zorg dragen voor een integrale aanpak van informatieveiligheid in het hoger onderwijs, in workshops en tijdens het CIO Café.

Paul Rullmann, voorzitter Wetenschappelijk Technische Raad van SURF, oud-bestuurder TUDelft, en Doekle Terpstra, voorzitter College van Bestuur Inholland, stonden stil bij aspecten van integrale veiligheid waarvoor bestuurders van instellingen voor hoger onderwijs zich geplaatst zien. Daarbij liepen ze de bouwtekeningen van het hoger onderwijs langs om zicht te krijgen op kwetsbaarheden en te beschermen belangen. Ze brachten in kaart hoe bestuurders in het hoger onderwijs uit oogpunt van compliance en control zichzelf de maat (kunnen) nemen bij kwesties als informatieveiligheid, privacywetgeving en kennisveiligheid. Op welke manieren zorgt een goed architect voor hoger onderwijs dat staat als een huis? Kortom: wat te doen als het tocht tussen voor- en achterdeur? Hoe zorgen zij ervoor dat het hang- en sluitwerk op orde is?!

Integrale veiligheid vraagt om goed bestuur

Als bestuurder moet je zorgen dat je systemen op orde zijn. Je bent immers integraal verantwoordelijk voor het resultaat van je instelling. Het hoger onderwijs maakt deel uit van het publieke domein en heeft een maatschappelijke opdracht. Hogescholen leiden jonge mensen op tot reflectieve en creatieve beroepsbeoefenaren en tot zelfredzame burgers, die vanuit individueel perspectief hun verantwoordelijkheid nemen. Soms danst men op smalle koordjes en zoeken studenten bij het afnemen van tentamens grenzen op of gaan ze er over heen. Dat dwingt bestuurders dan tot ongelooflijke strengheid bij het aanpakken van fraude en schendingen van integriteit. Op alle terreinen moeten bestuurders 'in control' zijn. Ze zijn aansprakelijk. Dat aansprakelijkheidsbewustzijn van bestuurders geldt temeer daar waar de veiligheid van studenten, personeel en de organisatie in het geding zijn. Niet alleen fysieke veiligheid, ook digitale veiligheid. Niemand wil immers de regie over zijn digitale voetafdruk kwijt raken, ook niet in het hoger onderwijs.

Rullmann en Terpstra vertelden hun verhaal over risicomanagement in het hoger onderwijs aan de hand van recente ontwikkelingen en geleerde lessen over informatieveiligheid, privacybescherming en cybersecurity. Welke risico's hebben zij gezien, waardoor werden die veroorzaakt, met welke gevolgen zijn ze geconfronteerd en hoe hebben ze die risico's beheersbaar gemaakt?

Ze pleiten voor een integrale veiligheidsinfrastructuur, zoals deze in het project Integraal Veilig Hoger Onderwijs wordt ontwikkeld voor hogescholen en universiteiten.



Handreiking voor signalering en begeleiding veiligheids- en leefstijlrisico's in het hoger onderwijs

Achtergrond

De afgelopen jaren heeft het Rijk voor verschillende sectoren - waaronder onderwijs - en professionals landelijke bewustwordingstrainingen aangeboden voor eerstelijns werkers, over de fenomenen 'radicalisering en polarisatie' en zogenaamde 'potentieel gewelddadige eenlingen' (PGE).

Tijdens deze trainingen is het bewustzijn over deze fenomenen versterkt en is het inzicht ontstaan dat om deze signalen vervolgens goed te kunnen beoordelen, een goede dreigingsinschatting te kunnen maken en een aanpak te kunnen bepalen meer nodig is dan bewustzijn van de risico's, ook in het hoger onderwijs.

Pilot

De Hogeschool Rotterdam heeft als eerste het initiatief genomen deze problematiek te agenderen binnen de eigen instelling om voor signalering, inschatting en aanpak van veiligheidsrisico's in het hbo een handreiking te ontwikkelen. Deze handreiking is in belangrijke mate gebaseerd op de ervaringen die zijn opgedaan in de Hogeschool Rotterdam waar een pilot is uitgevoerd. Hier werd op basis van een hogeschoolbrede dilemmasessie geconcludeerd dat een dergelijk plan van aanpak niet alleen van nut kan zijn voor het kanaliseren van de aanpak bij potentieel gevaarlijke eenlingen of radicalisering, maar ook kan dienen voor de signalering en aanpak van andere veiligheids- en leefstijlrisico's bij studenten in het hbo en zo indirect kan dragen aan het terugdringen van studie-uitval.

Uitkomst van de dilemmasessie:

"Er bestaat een duidelijke consensus over dat er meer structuur en regie nodig is in de wijze waarop signalen over veiligheids- en leefstijlvragen bij studenten worden gedeeld en aangepakt. Men wil nadrukkelijk dat signaleerders er niet alleen voor staan, maar bij collega's en experts ondersteuning kunnen vinden. Daarmee kunnen zij zich primair blijven richten op hun onderwijsgerelateerde taken, maar wordt ook bijgedragen aan een veilig schoolklimaat en betere voorwaarden voor een positieve studieloopbaan van studenten. Dit vraagt om betrokkenheid en inzet op alle niveaus; van de docent in de groep tot en met het CvB, ieder in zijn eigen rol."

Multidisciplinaire aanpak

Deze wens past nadrukkelijk in een bredere maatschappelijke context en veranderende beelden over de rol van het (hoger) onderwijs. Vanuit ARBO-wetgeving en landelijke campagnes rond de Veilige Publieke Taak staat de verantwoordelijkheid van werkgevers voor de veiligheid van haar personeel (en in het onderwijs daarmee meteen ook haar studenten) de laatste jaren sterk in de aandacht. Daarnaast zien veel Hogescholen hun studentenpopulatie de laatste jaren sterk veranderen naar een pluriforme doelgroep met een grote diversiteit en uiteenlopende culturele waarden. Dat stelt docenten en ander personeel voor ingewikkelder handelingsvragen op het gebied van gedrag en omgangsvormen. Maar ook neemt hiermee de complexiteit van de problematiek bij individuele studenten toe. En die problematiek komt ook de school binnen.

Breder inzetbaar

De urgentie om actiever te werken aan signalering en aanpak van veiligheids- en leefstijlrisico's wordt nog verhoogd door de invoering van de verplichte meldcode Huiselijk Geweld en Kindermishandeling, die per 1 juli 2013 van kracht is geworden. Ook professionals in instellingen voor hoger onderwijs zijn dan verplicht op te treden bij vermoedens van huiselijk geweld of kindermishandeling. Met het inrichten van een ondersteuningsstructuur wordt meteen een basis gelegd voor het voldoen aan de eisen van de verplichte Meldcode.

Voor meer informatie over de pilot en beleid en aanpak van de Hogeschool Rotterdam met betrekking tot veiligheids- en leefstijlrisico's: Paul Goossens, manager integrale veiligheid HR: p.a.m.goossens@hr.nl

De handreiking wordt op korte termijn beschikbaar gesteld op de website www.integraalveilig-ho.nl
Voor deskundigheidsbevordering op gebied van PGE: <https://toolbox-extremisme.nctv.nl/>



Meldcode Huiselijk geweld en kindermishandeling

Met ingang van 1 juli 2013 zijn beroepskrachten binnen onderwijsinstellingen, ook in het hoger onderwijs, verplicht een meldcode te gebruiken bij signalen van huiselijk geweld of kindermishandeling.

Een meldcode beschrijft in vijf stappen wat (bijvoorbeeld) een docent of leidinggevende moet doen bij een vermoeden van geweld:

1. In kaart brengen van signalen.
2. Overleggen met een collega en eventueel raadplegen van het Advies- en Meldpunt Kindermishandeling of het Steunpunt Huiselijk Geweld.
3. Gesprek met de (cliënt) leerling/student.
4. Wegen van het geweld of de kindermishandeling.
5. Beslissen: hulp organiseren of melden.

Eigen meldcode opstellen

Elke onderwijsinstelling maakt de meldcode specifiek voor de eigen praktijk. Bijvoorbeeld door te benoemen wie de stappen moet doorlopen. Zo kan een instelling afspreken dat de melder de signalen bespreekt met de vertrouwenspersoon. Ook kan het nodig zijn in de meldcode extra aandacht te besteden aan signalering en handelwijze bij specifieke vormen van geweld. Een model voor een meldcode is te vinden op Rijksoverheid.nl.

Meldcode wettelijk verplicht

Elke instelling voor hoger onderwijs (hbo, wo, bekostigd en niet-bekostigd) is verplicht om een meldcode te hebben (artikel 1.21 WHW). Vanaf augustus 2015 ziet de inspectie van het onderwijs bij alle onderwijsinstellingen toe op de naleving van dit wettelijke voorschrift. Vanuit het project Integrale Veiligheid Hoger Onderwijs wordt op korte termijn een handreiking beschikbaar gesteld op de website. www.integraalveilig-ho.nl

Zie verder: <http://www.onderwijsinspectie.nl/actueel/nieuwsbrieven/e-nieuws-hoger-onderwijs-november-2013.html>

Code goed bestuur hogescholen

Op 3 oktober hebben de hogescholen ingestemd met de Code goed bestuur die voortbouwt op de tot dan geldende Branchecode governance hbo. In de nieuwe code zijn de aanbevelingen verwerkt van de commissie Van Montfort, die in opdracht van het bestuur van de Vereniging Hogescholen de governancecode heeft geëvalueerd. Gebleven zijn de verplichting tot het hebben van een integriteitcode, een klokkenluiderregeling en een regeling ongewenst gedrag als onderdelen van een risicomanagement systeem. Nieuw in de Code goed bestuur is de verplichting voor het CvB om in het jaarverslag inzicht te geven in de werking en de belangrijkste resultaten van dat interne risicomanagementsysteem. Daarmee wordt een belangrijke kwaliteitsslag gemaakt in de transparantie van bestuur en toezicht. De tools en processen zijn aanwezig, nu gaat het erom te laten zien dat (en hoe) ze werken.

De Code goed bestuur staat op de website van de Vereniging Hogescholen: <http://www.vereniginghogescholen.nl/bedrijfsvoering/goed-bestuur>.



Veilig Internationalisering in het HO

Vanuit het Ministerie van OCW is de vraag gesteld in hoeverre internationalisering bij hoger onderwijs instellingen een veiligheidsrisico vormt. En zo ja, welke risico's zij lopen en welke maatregelen er getroffen zouden moeten worden. Op internet (<https://intranet.tudelft.nl/nl/citg/nieuws/artikel/detail/overvallen-in-mozambique/en> <http://delta.tudelft.nl/artikel/avontuur-in-afrika/26215>) kunt u een beschrijving van een incident met studenten van de TU Delft in Mozambique vinden en hoe de TU dit heeft aangepakt. Hier kunt u lezen dat het noodzakelijk is veilig internationaliseren op te nemen in uw integrale veiligheid maatregelen. Hieruit blijkt tevens dat er op het gebied van veiligheid voor studie- en werk gerelateerde activiteiten in het buitenland een aantal zaken universiteiten breed geregeld zouden kunnen worden zoals bijvoorbeeld een gezamenlijke verzekering, een gezamenlijke incidenten registratie- en crisismanagement systeem.

Het deelproject Integraal Veilig Internationaliseren (IVI wil dat voor bovengenoemde en andere risico's voor studenten en medewerkers (externe en interne mobiliteit) de juiste pro- en reactieve maatregelen op efficiënte en effectieve wijze worden ontwikkeld en uitgevoerd. Om dit te bereiken zijn de afgelopen tijd met behulp van het Bow Tie model de veel voorkomende risico's op het gebied van interne en externe mobiliteit met bijbehorende maatregelen in kaart gebracht.

Het proces

In oktober zijn er drie bijeenkomsten georganiseerd.

De eerste bijeenkomst is gehouden met studenten; Nederlandse studenten die enige tijd in het buitenland hebben gestudeerd en buitenlandse studenten die in Nederland een studie volgden. De tweede bijeenkomst is gehouden met Nederlandse medewerkers die enige tijd in het buitenland hebben gewerkt en buitenlandse medewerkers die in Nederland werkzaam zijn en de derde bijeenkomst is gehouden met experts die studenten en medewerkers in het buitenland begeleiden. Dit waren security specialisten, medewerkers van het International office en docenten die studenten in het buitenland begeleiden. Bij de uitnodiging van de groepen is rekening gehouden met een goede mix van hogescholen en universiteiten en de locatie van de instelling in Nederland.

De deelnemers aan de bijeenkomsten werden verdeeld in groepjes. De vragen die hen gesteld werden waren:

Welke incidenten heb je meegemaakt of van gehoord?

Wat was de schade die door het optreden van de incidenten ontstond?

Welke maatregelen zouden genomen moeten worden om te voorkomen dat een dergelijk incident nog eens optreedt?

Welke maatregelen moet je nemen om de schade, nadat het incident is opgetreden, te beperken?

Tijdens de bijeenkomsten werd eerst de aanpak, die wordt gehanteerd om de risico's en de maatregelen die deze risico's moeten beperken, uiteengezet.

Eerste resultaten

Het achterhalen van risico's die optreden bij extern en intern internationaliseren van het hoger onderwijs met behulp van groepsbijeenkomsten blijkt een effectieve aanpak te zijn.

Door deelnemers het theoretisch kader van de Bow Tie uit te leggen is men goed in staat dreigingen, gevolgen en preventieve en repressieve barrières op te sporen. Tijdens de bijeenkomsten bleek dat de dreigingen en incidenten voor studenten en medewerkers hetzelfde zijn. Het verschil tussen de twee groepen is dat medewerkers meer levenservaring hebben en vaker in staat zijn onheil te voorkomen en ook beter in staat zijn optredende problemen op te lossen. Er bestaat wel een duidelijk verschil tussen de risico's die Nederlandse studenten en medewerkers in het buitenland ondervinden en de risico's die buitenlandse studenten en medewerkers in Nederland ondervinden.

De aanpak heeft tot resultaat gehad dat er twee Bow Ties gemaakt zijn. Eén voor de Nederlandse studenten/medewerkers die naar het buitenland gaan (externe internationalisering) en één voor buitenlandse studenten/medewerkers die in Nederland komen studeren/werken (interne internationalisering).

Naar aanleiding van de analyses kan geconcludeerd worden dat studenten en medewerkers dezelfde risico's ondervinden. Wel is er een duidelijk verschil tussen de risico's die gepaard gaan met externe en interne internationalisering. De risico's zijn op een redelijke manier goed te beheersen. Alles hangt echter af van een goede voorbereiding voorafgaand aan het vertrek en een goede begeleiding.

Een belangrijke conclusie is dat medewerkers en studenten grote behoefte hebben aan een Engelstalige website waarop alle relevante informatie te vinden is die het verblijf in het buitenland kan veraangename en een website voor buitenlandse studenten in Nederland en een website voor Nederlandse studenten in het buitenland.

Bovendien kwam naar voren dat het handig is, een mogelijkheid te bieden, elektronisch vragen te stellen, wat een student of medewerker een hoop ellende kan besparen. Wel is het zaak dat vragen en suggesties serieus worden genomen en snel en adequaat worden beantwoord en afgehandeld. Ook is het belangrijk dat mensen via de websites hun ervaringen kunnen delen en suggesties kunnen doen om risico's te verkleinen.

Studenten en medewerkers die terugkeren in Nederland zouden ook een debriefing moeten krijgen zodat de onderwijsinstelling kan leren van hun ervaringen. Er bestaat bovendien een belangrijke behoefte bij de verschillende onderwijsinstellingen om ervaringen met elkaar te kunnen delen.

Met de opkomst van social media is het makkelijker om op eenvoudige wijze in contact te blijven met mensen die in het buitenland verkeren en in Nederland. Daarnaast bestaan er apps die actuele informatie geven over de politieke toestand in een bepaald land en de eventuele dreiging van natuurrampen.

Met dit document is de eerste stap gezet om te komen tot een risicomanagementsysteem voor de risico's die zich voordoen bij interne en externe internationalisering. De volgende belangrijke stap is de uitwerking en implementatie van de geïnventariseerde maatregelen. Nadat de resultaten zijn uitgewerkt zal er een handig handboek worden ontwikkeld, die de verschillende betrokken gremia binnen de hoger onderwijs instellingen kunnen helpen om het veiligheidsproces bij (interne en externe) internationalisering efficiënt en effectief te borgen. Om het handboek te verlevendigen zal binnenkort gestart worden met het opnemen van een korte maar aansprekelijke film over de risico's en maatregelen bij internationalisering, die bij het IVI Handboek wordt bijgeleverd.

Terugkomend op het voorbeeld: Als de proactieve maatregelen, zoals trainingen, verzekeringen, ambassade informatie, crisisproces "in place" zijn voorkom je veel.

