NETWERK IBP IN HET MBO

Kennisnet SURF saMBO-ICT

Netwerk informatiebeveiliging en privacy in het mbo
donderdag 16 mei 2019

Auteur Regiegroep ibp in het mbo
Datum 16 mei 2019

NETWERK IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Programma:

Inhoud

1. **Welkom, mededelingen Wim**
2. Terugkoppeling vanuit de werkgroepen
   - Verwerkersovereenkomsten
   - Update toetsingskaders
   - Dataregisters
3. Datalek, twee praktijkcases. Niels Dutij
4. Office 365, security en compliance tools
5. Pauze
6. Roept u maar!
7. Cyberdreigingsbeeld SURF, hoe zit dat in het mbo?
   - Presentatie van het cyberdreigingsbeeld. Bart en Maarten
   - Hoe ligt dat in het mbo?

NETWERK IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Inhoud

Programma:

1. Welkom, mededelingen Wim
2. **Terugkoppeling vanuit de werkgroepen**
   - **Verwerkersovereenkomsten**
   - **Update toetsingskaders**
   - **Dataregisters**
3. Datalek, twee praktijkcases. Niels Dutij
4. Office 365, security en compliance tools
5. Pauze
6. Roept u maar!
7. Cyberdreigingsbeeld SURF, hoe zit dat in het mbo?
   - Presentatie van het cyberdreigingsbeeld. Bart en Maarten
   - Hoe ligt dat in het mbo?

Nr.	Leverancier/applicatie
2018/12	**Exact** (Merces)
2018/33	**Topdesk,** is klaar, december 2018
	ICE
2018/1	**ADP**, deze wordt niet gescreend door de werkgroep, er is maar 1 ROC dat deze applicatie voert en SURF gaat de screening wellicht doen in de nabije toekomst
	Microsoft, voor Microsoft worden de huidige overeenkomsten van SURF gebruikt. Er lopen gesprekken om deze te vernieuwen.
	Google, er lopen gesprekken met Google om tot overeenkomsten te komen
	Inspectie en accountant, zie de FAQ vraag 13
2018/9	**Deviant**, is klaar, juni 2018
2018/34	**Trajectplanner/Fringe,** is klaar, december 2018
2018/2	**AFAS HRM/Payroll**, is klaar, december 2018
2018/1	**AFAS Financieel**, is klaar, december 2018
2018/24	**Magister**, is klaar, december 2018
2018/29	**Ricoh:** Ricoh werkt meestal on premise, dan is er geen verwerkersovereenkomst nodig, hooguit een geheimhoudingsverklaring bij onderhoudsactiviteiten. Werkt het niet on premise, dan gaat Ricoh akkoord met de artikelen uit de modelovereenkomst 3.0 en moet er voor elke instelling specifiek een bijlage opgesteld worden.
	Fronter
2018/16	**GP Untis**, klaar februari 2019
2018/31	**TIG/Qlickview**, klaar december 2018
2018/18	**Ibabs,** klaar februari 2019
2018/10	**Eduarte**, klaar juli 2018
	It's Learning (i.s.m. PO groep)
2018/28	**Raet,** is klaar, juli 2018
2018/21	**Intergrip,** is klaar, augustus 2018
2018/	**Effectory**, is klaar, mei 2018
2018/	**ExSamen**, de vereniging ExSamen is in mei toegetreden tot het Privacy Convenant 3.0, alle leveranciers zullen zich aan het model 3.0 gaan houden **SPL (Stichting Praktijk Leren)** heeft als eerste leverancier van de vereniging het model 3.0 overgenomen, is klaar, februari 2019
2018/7	**Cum Laude/N@tschool,** klaar 16 juli 2018
2018/8	**Acknowledge**, hostingspartner voor Cum Laude, klaar december 2018
2018/35	**Xedule/Advitrae**, klaar juni 2018
2018/17	**HR2Day,** is klaar, december 2018
2018/3	**AMN**, klaar juli 2018
2018/30	**SURFfilesender,** loopt via SIRFmarket, zie ook FAQ lijst
2018/6	**CITO,** is klaar, juli 2018
2018/32	**Tools4Ever,** is klaar, december 2018

Werkgroep verwerkers-overeenkomsten:

4 juni overleg over continuering van de werkgroep

Eventueel:

- vragen vanuit instellingen
- Audits bij leveranciers
- …..

Update toetsingskaders:

Toetsingskader privacy
- Job en Peter maken afspraak met werkgroepje

Toetsingskader examinering
- In progress
- Nieuwe formulering en indeling (PE)
- Afronding 11 juni klankbordgroep examinering mbo

Toetsingskader ib vs 4.0
- Presentatie Ludo

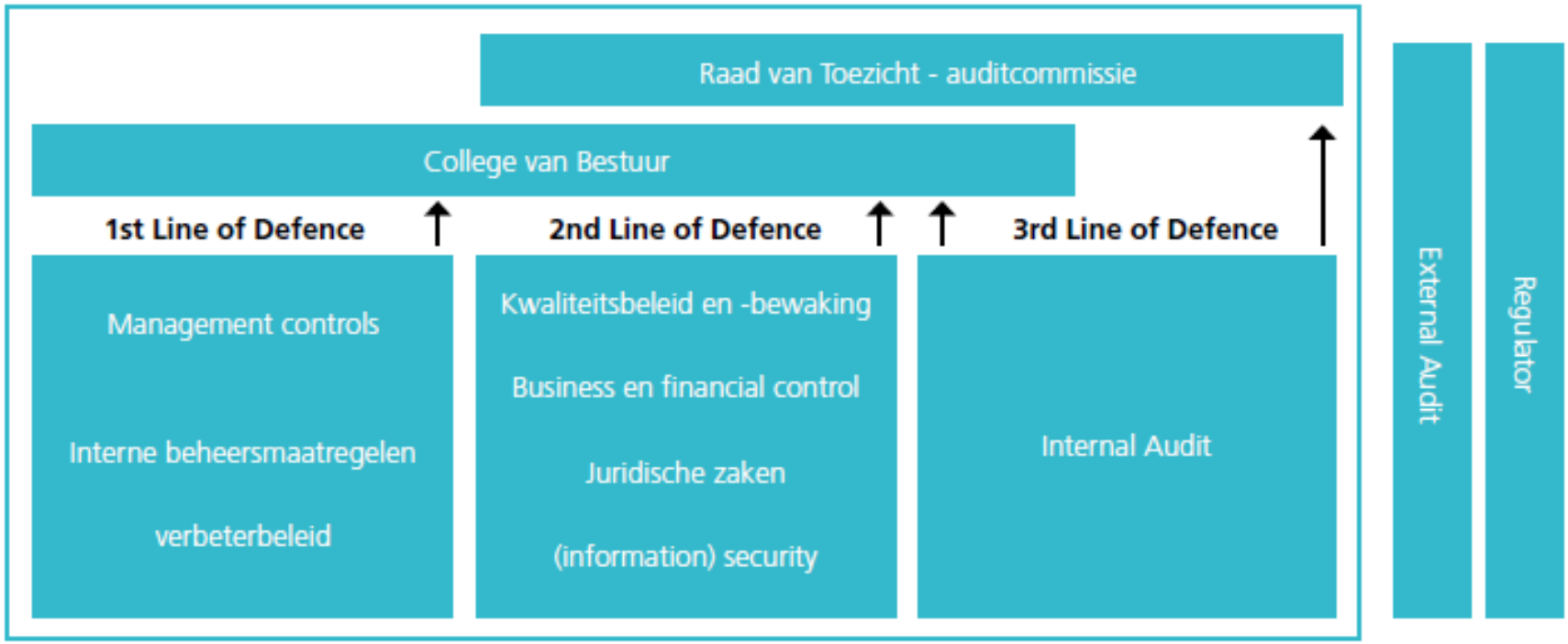
Kennisnet

Netwerkbijeenkomst
16-5-2019

Kennisnet

4	College van Bestuur: **Verwerkingsverantwoorlijke**
3	FG, IT auditor en RvT: **Toezichthouder**
2	CISO en Privacy officer: **Ondersteuner**
1	Managers, Informatie managers, Hoofd Inkoop, ICT medewerkers (netwerk en applicatie beheer) en “nog te benoemen”: **Uitvoerder IBP beleid**

4 lines of defence
IBP-beleid ROC Nijmegen


Raad van Toezicht - auditcommissie
College van Bestuur
1st Line of Defence
2nd Line of Defence
3rd Line of Defence
Management controls
Interne beheersmaatregelen
verbeterbeleid
Kwaliteitsbeleid en -bewaking
Business en financial control
Juridische zaken
(information) security
Internal Audit
External Audit
Regulator


IBP risico's (Cyberdreigingsbeeld)
Nieuwe projecten
IBP jaarplan
Scholing en awareness
Dataregisters 1.0
Medewerker
Student/leerling
Relatie
Wetenschappelijk onderzoek vrijwilliger
DPIA
SURF pré DPIA
DPIA Rijksoverheid
PIA NOREA
PbD / Aanbesteding
Verwerkers-overeenkomsten
Dataregisters 1.1
IBP beleid
Richtlijnen
Compliance
Governance
Incidenten beheer
Toetsingskader NBA
Beleid
Audit
Techniek
Toetsingskader 4.0 b
Cluster 7 (privacy)
Autorisatie
Autorisatiematrices
Dataclassificatie
Pentest

Kennisnet

Niveau 1: Initieel

Ad hoc

Beheersingsmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen.

Geen of beperkte controls geïmplementeerd.
Niet of ad-hoc uitgevoerd.
Niet /deels gedocumenteerd.
Wijze van uitvoering afhankelijk van individu.

Kennisnet

Niveau 2: Herhaalbaar

Opzet, bestaan en beperkte werking

Beheersingsmaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar op informele wijze uitgevoerd.

Control is geïmplementeerd.
Uitvoering is consistent en standaard.
Informeel en grotendeels gedocumenteerd.

Kennisnet

Niveau 3: Gedefinieerd
Uitgebreide werking

Beheersingsmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst.

Control gedefinieerd o.b.v. risico assessment.
Gedocumenteerd en geformaliseerd.
Verantwoordelijkheden en taken eenduidig toegewezen.
Opzet, bestaan en effectieve werking aantoonbaar.
Rapportage van uitvoering van beheersingsmaatregel aan management.
Effectieve werking van controls wordt periodiek getoetst, gebaseerd op het risicoprofiel van de organisatie.
De toetsing toont aan dat de control effectief is.

Kennisnet

Niveau 4: Beheerst en meetbaar
PDCA

De effectiviteit van de beheersingsmaatregelen wordt periodiek geëvalueerd.

Periodieke (control) evaluatie en opvolging vindt plaats.
Evaluatie is gedocumenteerd en geformaliseerd.
Frequentie waarop wordt geëvalueerd is gebaseerd op het risicoprofiel van de onderneming en is minimaal jaarlijks.
Rapportage van de evaluatie aan management.

Logo mbo instelling (MI)

Register van de verwerkingsactiviteiten (Data register) Artikel 30 AVG

Dataregister 1

versie 2.2, 17-10-20[illegible]

A		
Contactgegevens van XX	Verwerkingsverantwoordelijke:	Contactgegevens Functionaris voor de Gegevensbescherming	Loket privacy informatie (optioneel):
	XX (voorzitter College van Bestuur)	xx@xx.nl	Bijvoorbeeld: studenten administratie
	Gemandateerd: XX (bijvoorbeeld Directeur Bedrijfsvoering)	www.xx.nl	

B	C		H
Categorie van de betrokkene: **Student**	Verwerkingsdoeleinden:	Grondslag van de verwerkingsdoel[einden]	Doorgifte van persoonsgegevens b[uiten de EER]
	a. Komen tot een Onderwijsovereenkomst (OOK)	→ Wettelijk en overeenkomst	Geen persoonsgegevens buiten de EER.
	b. Komen tot een Praktijkovereenkomst (POK)	→ Wettelijk en overeenkomst	
	c. Verantwoorden aan DUO, Inspectie en Accountant (bijlage OOK)	→ Wettelijk	
	d. Voorbereiden voor aanschaf (digitale) leermiddelen	→ Gerechtvaardigd belang	
	e. Pedagogisch dossier (overleg, examineren en aanwezigheid registra[tie])	→ Wettelijk en overeenkomst	
	f. Uitvoering of toepassing van een andere wet	→ Wettelijk	

J Algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen	E	Brondocumenten	I Bewaartermijnen
Voorbeeld: Basisniveau uitgevoerd op de informatiebeveiliging (ISO 27002), beoordeling volwassenheidsniveau 2,5 op basis van Toetsingskader SURF (schaal 1-5). Beoordeling uitgevoerd op Privacy (AVG2018), beoordeling volgt.	I	Digitale aanmelding	2 of 7 jaar na beëindiging OOK
	II	Kopie of image id/paspoort of DigiD	Maximaal 1 maand
	III	[illegible]	2 of 7 jaar na beëindiging OOK
	IV	Overdrachtsinformatie	2 jaar na beëindiging OOK
	V	Verslag intakegesprek (-AMN)	2 jaar na beëindiging OOK
	VI	Specifieke documenten	2 of 7 jaar na beëindiging OOK

G	Verwerkersovereenkomsten			
	naam	omschrijving	Website informatie	Datalocatie
1	SIS: Magister	Studenten Informatie Systeem	www.magister.nl	Hengelo
2	ELO: Fronter	Elektronische Leer Omgeving	www.fronter.nl	Oslo (Noorwegen)
3	MIS: Qlikview	Management Informatie systeem	www.qlikview.nl	Amsterdam
DS	Dataregisterbeheer	Uitwerking Toets, Roosters, Overig en IDM		
4	St. Collectief Jongeren Paspoort	CJP-pas	www.cjp.nl	Amsterdam

D Categorieën van persoonsgegevens (categorie 13 niet in gebruik)	F Externe verwerkersverantwoordelijken: DUO inschr	DUO exam	DUO BPV	DUO VSV	INSP	JOB	BPV	Accountant	G Verwerkers: SIS 1	ELO 2	MIS 3	Toets DS	[illegible] DS	CJP 4	Applicaties op locatie: FIN 4	CRM 5	IDM DS	XX Toegangsrechten tot persoonsgegevens: Stud. Admin	Opleiding	Financiën	ICT faciliteit	Zorg/intake	BIV
	W	W	W	W	W	T	W	W	V/V/W	•	•	•	•	•	W	•	•	•	•	•	•	•	
1a Contactgegevens: naam, e-mail en org.eenheid	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	H-M-H
1b Contactgegevens: geboortedatum en geslacht	X	X	X	X	X	X	X	X	X	X	X	X		X	X			X	X	X		X	H-M-H
1c Contactgegevens: overige gegevens	X	X	X	X	X		X	X	X	X	X	X		X	X	X		X	X	X		X	H-M-H
2 Studentnummer	X	X	X	X				X	X	X	X	X	X	X	X	X	X	X	X	X		X	H-M-H
3 Nationaliteit en geboorteplaats	X							X	X					X	X			X				X	H-M-H
4 Ouders of voogd	X				X			X	X						X			X	X			X	H-M-H
5 Gezondheidsgegevens (op eigen verzoek)									X									X	X			X	H-M-H
6 Godsdienst (op eigen verzoek)									X									X				X	H-M-H
7 Studievoortgang: 7a Examinering		X			X		X	X	X	X	X	X						X	X	X		X	H-M-H
7 Studievoortgang: 7b Trajectoverleg					X		X	X	X	X								X	X	X		X	H-H-H
7 Studievoortgang: 7c Begeleiding Student					X			X	X				X					X	X	X		X	H-H-H
7 Studievoortgang: 7d Aanwezigheidsregistratie					X		X	X	X				X					X	X	X		X	H-M-H
7 Studievoortgang: 7e Medisch dossier																						X	H-M-M
8 Onderwijsorganisatie (roosters, boekenlijst, etc.)									X									X	X			X	H-H-H
9 Financiën [illegible]									X						X			X	X	X		X	H-M-H
10 Beeldmateriaal																		X	X				H-M-M
11 Docenten, mentoren en slb adviseur			X						X	X	X		X			X	X	X	X			X	H-M-H
12 BSN	X	X	X	X	X		X	X	X			X						X	X			X	H-M-M
14 Overige gegevens									X										X			X	H-M-H

FOKKE & SUKKE

MOETEN DIT DOEN VAN HUN BAAS

Peer review onderzoek

Aanleiding
Afgelopen jaar hebben 57 onderwijsinstellingen deelgenomen aan de benchmark Informatiebeveiliging, Privacy en Examinering. De resultaten zijn hieronder weergegeven:

	2015	2016	2017	2018
Cluster 1: Beleid en organisatie	1,7	1,8	2,0	2,4
Cluster 2: Personeel, studenten en gasten	1,7	1,7	1,9	2,3
Cluster 3: Ruimtes en apparatuur	2,1	2,2	2,3	2,5
Cluster 4: Continuïteit	2,0	2,1	2,3	2,5
Cluster 5: Vertrouwelijkheid en integriteit	2,0	2,0	2,2	2,4
Cluster 6: Controle en Logging	1,6	1,6	1,8	2,1
Totaal score Informatiebeveiliging in de mbo sector	1,9	1,9	2,1	2,4
Totaal score Privacy in de mbo sector	-	1,5	1,9	2,3
Totaal score Examinering in de mbo sector	-	-	-	2,1
Deelnamepercentage	29%	46%	77%	95%

Als sector willen we ook graag weten of deze scores betrouwbaar zijn. In dat kader hebben de mbo instellingen zich kunnen inschrijven voor een peer review. De opzet van een dergelijke peer review is dat een collega met kennis van informatiebeveiliging en privacy van een mbo instelling een andere mbo instelling toetst op de juistheid van de ingevulde volwassenheidsniveaus. Een deel van de statements (10 van de 85) zijn daarbij onderzocht en terug gerapporteerd in een zogenaamd "Rapport van bevindingen". De deelnemers zijn vooraf getraind en de rapporten zijn gelezen en van commentaar voorzien door een externe (gecertificeerde) IT auditor.
In totaal hebben 10 mbo instellingen van dit aanbod gebruik gemaakt.

Bevindingen
- 8 mbo instellingen hebben uiteindelijk een rapport opgeleverd aan de mbo instelling die zij hebben onderzocht.
- Van de 80 onderzochte statements waren 24 te hoog gewaardeerd.
- Er is niet onderzocht of er statements te laag gewaardeerd waren.
- De rapporten waren van een goede kwaliteit in het licht van de peer review gedachte, maar onder de maat als audit rapport.

Aanbevelingen
Om de kwaliteit van de audit-verbetercyclus in het mbo ten aanzien van het self-assessment en de peer-review te verhogen zijn de volgende aanbevelingen van belang:

- Agendeer het onderwerp informatiebeveiliging & privacy op de bestuurlijke agenda van Kennisnet en de MBO-raad om ervoor te zorgen dat de audit-verbetercyclus als kwaliteits-proces wordt verankerd in de mbo-sector. Hierdoor wordt bewerkstelligd dat de resultaten van het self-assessment betrouwbaarder worden en geeft dit meer inzicht welke problemen in welke statements mbo-breed spelen. Deze mbo-brede knelpunten kunnen dan in gezamenlijkheid worden opgepakt binnen de sector.
- Train de auditors die een peer-review uitvoeren in de methodiek van het auditen en het schrijven van een peer-review-rapportage in de 'IT-audit taal'. De kwaliteit van de peer-review-rapportages is onder de maat, als audit rapport, waardoor de resultaten niet eenduidig zijn en er ruimte is voor interpretatie. Hierdoor zijn resultaten niet altijd eenduidig te vergelijken.
- In de gekozen auditmethodiek wordt alleen gekeken of een volwassenheidniveau wel of niet is aangetoond. Om tot een completer volwassenheidsbeeld te komen is het van toegevoegde waarde om in het oordeel ook mee te nemen of een volwassenheidsniveau hoger had kunnen zijn.
- Het aantal van 8 deelnemers is te laag om een uitspraak te doen voor de hele sector. Statistische is er sprake van een deelwaarneming en geen steekproef. Het is wenselijk dat 15 tot 20 mbo instellingen deelnemen om te komen tot en getrouw beeld.

Peer Review:

3e ronde opgestart

10 deelnemers

Afronding direct na de zomervakantie

Volgend jaar een caroussel inrichten?

Andere werkzaamheden:

Handreiking FG… binnenkort

FAQ werkgroep gestart

DPIA werkgroep gestart

Model ibp beleid, IBPDOC6

Aanpak ibp in het PO/VO gelanceerd

Aanpak ibp in het mbo, update arrangement

Vragen

???

NETWERK IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Programma:

Inhoud

1. Welkom, mededelingen Wim
2. Terugkoppeling vanuit de werkgroepen
   - Verwerkersovereenkomsten
   - Update toetsingskaders
   - Dataregisters
3. **Datalek, twee praktijkcases. Niels Dutij**
4. Office 365, security en compliance tools
5. Pauze
6. Roept u maar!
7. Cyberdreigingsbeeld SURF, hoe zit dat in het mbo?
   - Presentatie van het cyberdreigingsbeeld. Bart en Maarten
   - Hoe ligt dat in het mbo?

NETWERK IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Inhoud

Programma:

1. Welkom, mededelingen Wim
2. Terugkoppeling vanuit de werkgroepen
   - Verwerkersovereenkomsten
   - Update toetsingskaders
   - Dataregisters
3. Datalek, twee praktijkcases. Niels Dutij
4. **Office 365, security en compliance tools, Harold van der Kamp**
5. Pauze
6. Roept u maar!
7. Cyberdreigingsbeeld SURF, hoe zit dat in het mbo?
   - Presentatie van het cyberdreigingsbeeld. Bart en Maarten
   - Hoe ligt dat in het mbo?

Pauze van +/- 15 minuten

NETWERK IBP IN HET MBO

Kennisnet SURF saMBO-ICT

NETWERK IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Programma:

Inhoud

1. Welkom, mededelingen Wim
2. Terugkoppeling vanuit de werkgroepen
   - Verwerkersovereenkomsten
   - Update toetsingskaders
   - Dataregisters
3. Datalek, twee praktijkcases. Niels Dutij
4. Office 365, security en compliance tools,
5. Pauze
6. **Roept u maar!**
7. Cyberdreigingsbeeld SURF, hoe zit dat in het mbo?
   - Presentatie van het cyberdreigingsbeeld. Bart en Maarten
   - Hoe ligt dat in het mbo?

NETWERK IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Inhoud

Programma:

1. Welkom, mededelingen Wim
2. Terugkoppeling vanuit de werkgroepen
   - Verwerkersovereenkomsten
   - Update toetsingskaders
   - Dataregisters
3. Datalek, twee praktijkcases. Niels Dutij
4. Office 365, security en compliance tools,
5. Pauze
6. Roept u maar!
7. **Cyberdreigingsbeeld SURF, hoe zit dat in het mbo?**
   - **Presentatie van het cyberdreigingsbeeld. Bart en Maarten**
   - **Hoe ligt dat in het mbo?**

Korte terugkoppeling en afronding. Borrel en buffet