NETWERK IBP IN HET MBO

Kennisnet SURF saMBO-ICT

Netwerk informatiebeveiliging en privacy in het mbo
donderdag 12 maart 2020

Auteur Regiegroep ibp in het mbo
Datum 12 maart 2020

NETWERK IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Het netwerkprogramma voor 12 maart:

Inhoud

1. Welkom, mededelingen
2. Terugkoppeling vanuit de werkgroepen
3. Kerstverhalen uit Maastricht, door Bart van den Heuvel, CISO UM
4. Pauze
5. Roept u maar!
6. Naar aanleiding van de Benchmark IBP/E mbo 2019
7. Controle en logging, dat moet beter!
8. In werkgroepen bespreken van het thema
9. Terugkoppeling en adviezen vanuit de werkgroepen
10. Afronding, buffet, informeel netwerken.

NETWERK IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Het netwerkprogramma voor 12 maart:

Inhoud

1. Welkom, mededelingen
   - App checker online, https://aanpakibp.kennisnet.nl/appchecker/
   - Politie brengt tool cybercrime uit, https://www.playframed.nl
   - Bestuurdersconferentie cybersecurity 15 april
   - Kamerbrief
   - Contact mbo - AP
   - OZON 2020
   - DPIA Microsoft
2. Terugkoppeling vanuit de werkgroepen
   - Verwerkersovereenkomsten
   - Awareness
   - DPIA
   - Regiegroep: netwerkomgeving MS-Teams
3. Kerstverhalen uit Maastricht, door Bart van den Heuvel, CISO UM
4. Pauze

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:

Wordt gecontinueerd, samenstelling gelijk, Ludo voorzitter

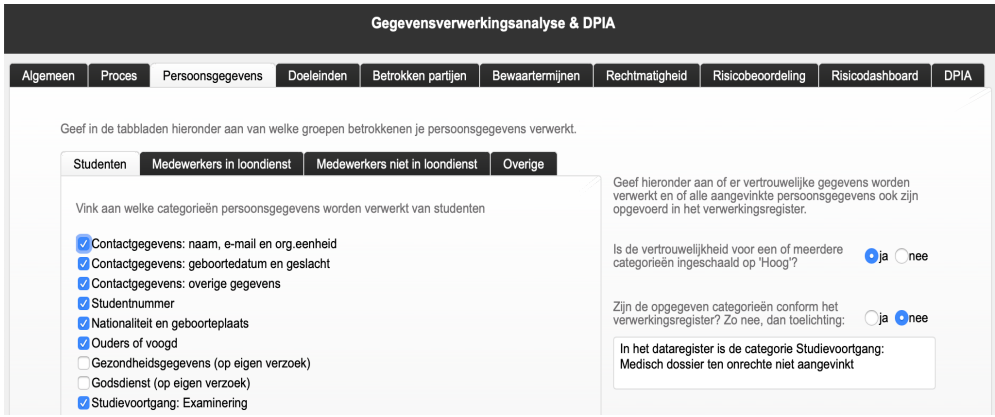
- Nieuwe aanvragen vwo's vanuit instellingen
- vraagbaak voor instellingen
- Audits bij leveranciers

Werkgroep
Awareness

Fung Yee
Willem
Helma

DPIA aanpak

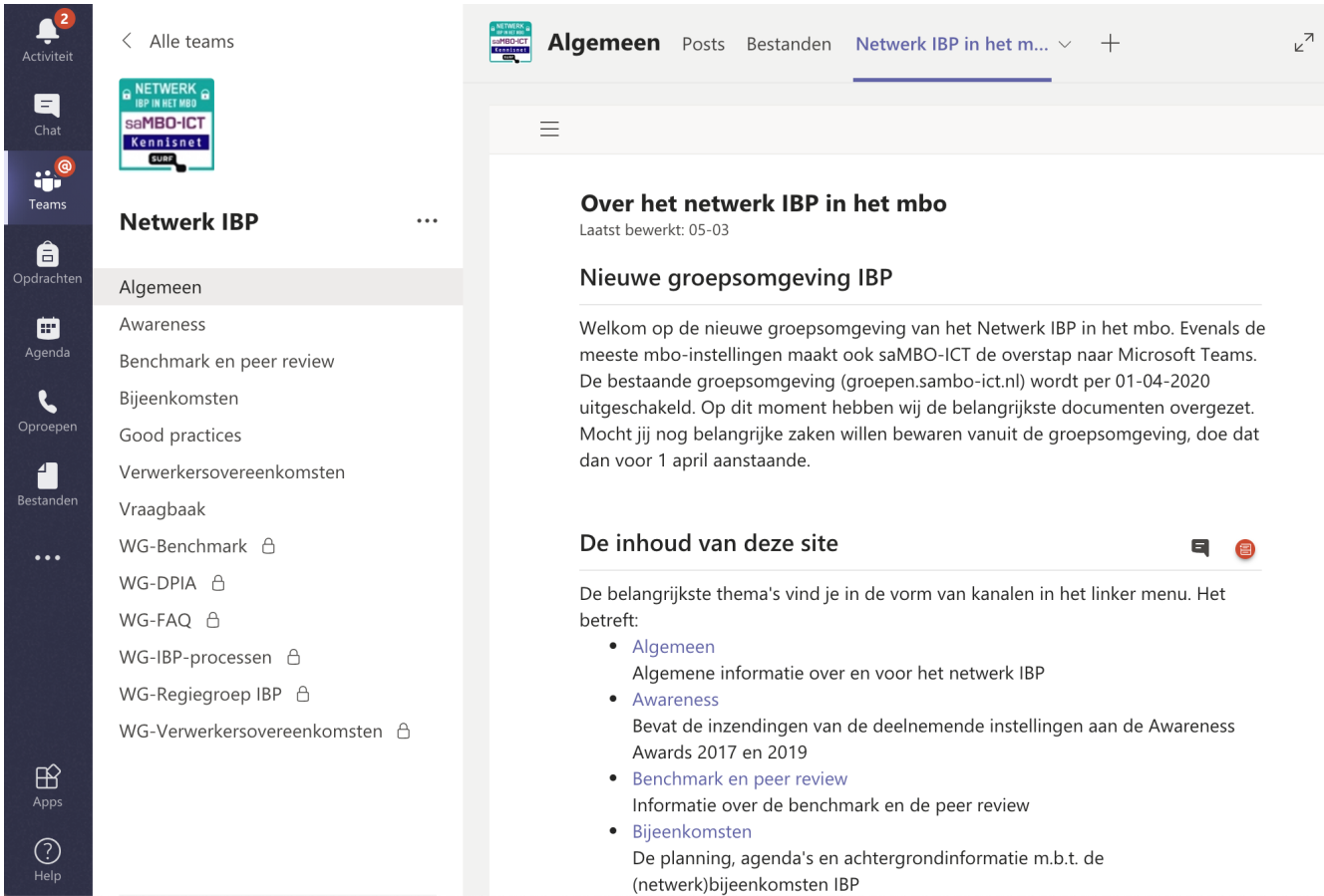
- Werkgroep: Willem, Bram, Bart, Martijn
- Twee stappen
  1. Gegevensverwerkingsanalyse
     - applicatielandschap
     - beschrijving verwerking
     - beoordeling rechtmatigheid
     - globale risicoanalyse
  2. DPIA
     - GVA
     - uitgebreide risicoanalyse
     - maatregelen
- Model-aanpak
  - Prototype in MS-Forms
  - Ook interesse vanuit PO/VO: opnemen in Aanpak IBP
  - Off-line testen bij de LAS-DPIA's voor PO/VO
  - Zo mogelijk door-ontwikkelen als database
  - Gegevens breed delen via DPIA-platform
    - van en voor de sector
    - vergelijkbaar met aanpak verwerkersovereenkomsten



Regiegroep ibp in het mbo:

De vernieuwde netwerkomgeving

- Van saMBO-ICT groepsomgeving naar MS Teams
- Gevolgen?
- Afspraken?



Vragen

???

REGIEGROEP IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Kerstverhalen uit Maastricht……

Ervaringen van een bijzondere kerstvakantie van Bart van den Heuvel, CISO Universiteit van Maastricht

Pauze van +/- 30 minuten

NETWERK IBP IN HET MBO

Kennisnet SURF saMBO-ICT

NETWERK IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Het netwerkprogramma voor 12 maart:

Inhoud

5. **Roept u maar!**
6. Naar aanleiding van de Benchmark IBP/E mbo 2019
   - SURF benchmark
   - Werkgroep ibp-processen
   - Update toetsingskader
   - Van 2.5 naar 3.0
   - Peer review
7. Controle en logging, dat moet beter!
   - Urgentie
   - Waar hebben we het over?
   - Uitstapje naar de ict-opleidingen.
   - SURF over cyberdreiging

NETWERK IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Het netwerkprogramma voor 12 maart:

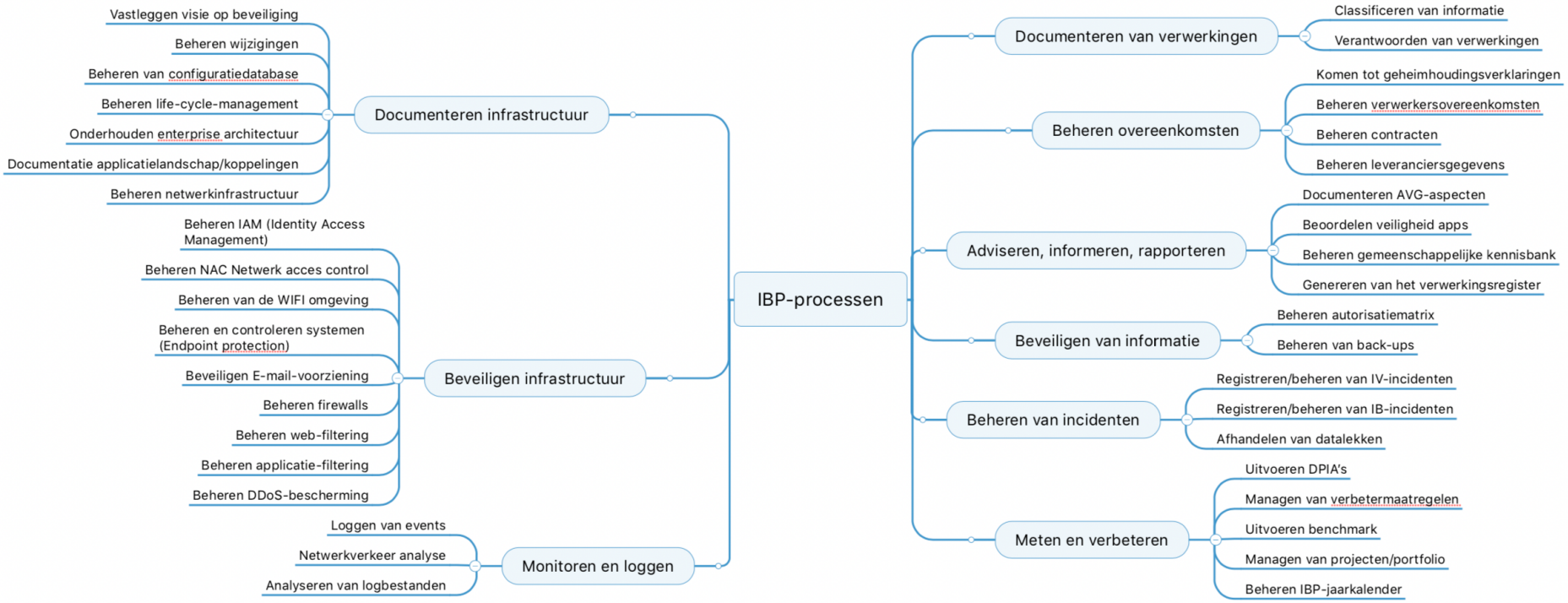
Inhoud

5. Roept u maar!
6. **Naar aanleiding van de Benchmark IBP/E mbo 2019**
   - Werkgroep ibp-processen
   - Update toetsingskader
   - Van 2.5 naar 3.0
   - Peer review
7. Controle en logging, dat moet beter!
   - Urgentie
   - Waar hebben we het over?
   - Uitstapje naar de ict-opleidingen.
   - SURF over cyberdreiging

REGIEGROEP IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Werkgroep ibp-processen

eerste inventarisatie



Werkgroep Update toetsingskader

Periode mei/juni 2020
- check op beschrijving/toelichting bewijsvoering IB
- wie doet mee?

Fung Yee Poon, Martijn Bijleveld

Controledoelstelling: Verwijdering van bedrijfsmiddelen Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring.
Toelichting: Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen. (Er is duidelijk vastgesteld wie vanuit welke rol toestemming hebben om apparatuur mee te nemen of buiten de locatie te gebruiken. Er zijn tijdslimieten en bij inlevering wordt gecontroleerd op de naleving daarvan. Waar nodig wordt geregistreerd wat de locatie verlaat en wanneer het weer wordt teruggebracht.)
Bewijsvoering: Het document "Verantwoord Netwerk Gebruik" (met daarin gebruik bedrijfsmiddelen) is opgenomen in het IBP-beleid in het hoofdstuk 3: Compliance.
2 Overleg het document "Verantwoord Netwerk Gebruik".
3 Overleg een print-screen waaruit blijkt dat het document "Verantwoord Netwerk Gebruik" eenvoudig te raadplegen en te downloaden is.

Van 2.5 naar 3.0

Ondersteuningsaanbod voor instellingen < 2.0
Onderzoek laag gescoorde statements
Focus op cluster 6 ‘Controle en logging’
Focus bij de bestuurders op IBP

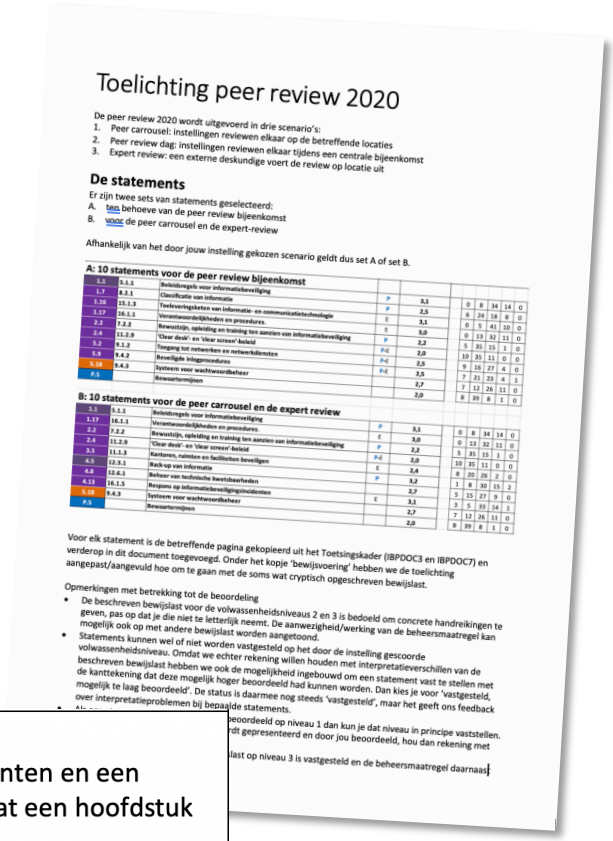
Regiegroep, Leo

Peer Review 2020

Plm 40 instellingen doen mee!
Vanaf nu tot 17 april

Drie scenario's:

1. Peer carrousel
2. Peer review dag
3. Expert review



Toelichting peer review 2020

De peer review 2020 wordt uitgevoerd in drie scenario's:

1. Peer carrousel: instellingen reviewen elkaar op de betreffende locaties
2. Peer review dag: instellingen reviewen elkaar tijdens een centrale bijeenkomst
3. Expert review: een externe deskundige voert de review op locatie uit

De statements

Er zijn twee sets van statements geselecteerd:

A. tav behoeve van de peer review bijeenkomst
B. voor de peer carrousel en de expert-review

Afhankelijk van het door jouw instelling gekozen scenario geldt dus set A of set B.

A: 10 statements voor de peer review bijeenkomst

5.1	5.1.1	Beleidsregels voor informatiebeveiliging	P	3,1	
1.7	8.2.1	Classificatie van informatie	P	2,5	
1.16	25.1.3	Toeleveringsketen van informatie- en communicatietechnologie	E	3,1	
1.17	26.1.1	Verantwoordelijkheden en procedures.	E	3,0	
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	P	2,2	
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	P-E	2,0	
5.2	6.1.2	Toegang tot netwerken en netwerkdiensten	P-E	2,5	
5.9	9.4.2	Beveiligde inlogprocedures	P-E	2,5	
5.18	9.4.3	Systeem voor wachtwoordbeheer		2,7	
P.5		Bewaartermijnen		0,0	

B: 10 statements voor de peer carrousel en de expert review

5.1	5.1.1	Beleidsregels voor informatiebeveiliging	P	3,1	
1.17	26.1.1	Verantwoordelijkheden en procedures.	E	3,0	
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	P	2,2	
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	P-E	2,0	
3.5	11.1.3	Kantoren, ruimten en faciliteiten beveiligen	E	2,4	
4.5	12.3.1	Back-up van informatie	P	3,2	
4.8	12.4.1	Beheer van technische kwetsbaarheden		2,7	
4.13	16.1.5	Respons op informatiebeveiligingsincidenten	E	3,1	
5.18	9.4.3	Systeem voor wachtwoordbeheer		2,7	
P.5		Bewaartermijnen		2,0	

Voor elk statement is de betreffende pagina gekopieerd uit het Toetsingskader (IBPDOC3 en IBPDOC7) en verderop in dit document toegevoegd. Onder het kopje 'bewijsvoering' hebben we de toelichting aangepast/aangevuld hoe om te gaan met de soms wat cryptisch opgeschreven bewijslast.

Opmerkingen met betrekking tot de beoordeling

- De beschreven bewijslast voor de volwassenheidsniveaus 2 en 3 is bedoeld om concrete handreikingen te geven, pas op dat je die niet te letterlijk neemt. De aanwezigheid/werking van de beheersmaatregel kan mogelijk ook op met andere bewijslast worden aangetoond.
- Statements kunnen wel of niet worden vastgesteld op het door de instelling gescoorde volwassenheidsniveau. Omdat we echter rekening willen houden met interpretatieverschillen van de beschreven bewijslast hebben we ook de mogelijkheid ingebouwd om een statement vast te stellen met de kanttekening dat deze mogelijk hoger beoordeeld had kunnen worden. Dan kies je voor 'vastgesteld, mogelijk te laag beoordeeld'. De status is daarmee nog steeds 'vastgesteld', maar het geeft ons feedback over interpretatieproblemen bij bepaalde statements.

Bewijsvoering: Niveau 2: Er is een procedure voor registratie van informatiebeveiligings- en privacy-incidenten en een procedure melding datalekken, mogelijk gecombineerd in 1 procedure. Het IBP-beleid bevat een hoofdstuk hierover of een verwijzing naar een document/richtlijn waarin het afhandelen van informatiebeveiligingsincidenten en datalekken is beschreven. Niveau 3: Maak aannemelijk dat alle hierbij betrokken medewerkers op de hoogte zijn van deze procedure(s) en/of laat zien aan de hand van bijvoorbeeld screenshots van het incidentregistratiesysteem dat de procedures zijn gevolgd.
2 Overleg het hoofdstuk van het IBP-beleid, waarin het afhandelen van informatiebeveiligingsincidenten en datalekken is vastgesteld.
3 Overleg een document waarin alle medewerkers in kennis zijn gesteld van het beleid met betrekking tot het afhandelen van informatiebeveiligingsincidenten en datalekken.

Peer Review 2020

A: 10 statements voor de peer review bijeenkomst										
1.1	5.1.1	Beleidsregels voor informatiebeveiliging	P	3,1		0	8	34	14	0
1.7	8.2.1	Classificatie van informatie	P	2,5		6	24	18	8	0
1.16	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	E	3,1		0	5	41	10	0
1.17	16.1.1	Verantwoordelijkheden en procedures.	E	3,0		0	13	32	11	0
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	P	2,2		5	35	15	1	0
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	P-E	2,0		10	35	11	0	0
5.2	9.1.2	Toegang tot netwerken en netwerkdiensten	P-E	2,5		9	16	27	4	0
5.9	9.4.2	Beveiligde inlogprocedures	P-E	2,5		7	21	23	4	1
5.18	9.4.3	Systeem voor wachtwoordbeheer		2,7		7	12	26	11	0
P.5		Bewaartermijnen		2,0		8	39	8	1	0

B: 10 statements voor de peer carrousel en de expert review										
1.1	5.1.1	Beleidsregels voor informatiebeveiliging	P	3,1		0	8	34	14	0
1.17	16.1.1	Verantwoordelijkheden en procedures.	E	3,0		0	13	32	11	0
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	P	2,2		5	35	15	1	0
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	P-E	2,0		10	35	11	0	0
3.5	11.1.3	Kantoren, ruimten en faciliteiten beveiligen	E	2,4		8	20	26	2	0
4.5	12.3.1	Back-up van informatie	P	3,2		1	8	30	15	2
4.8	12.6.1	Beheer van technische kwetsbaarheden		2,7		5	15	27	9	0
4.13	16.1.5	Respons op informatiebeveiligingsincidenten	E	3,1		3	5	33	14	1
5.18	9.4.3	Systeem voor wachtwoordbeheer		2,7		7	12	26	11	0
P.5		Bewaartermijnen		2,0		8	39	8	1	0

Peer Review 2020

Peer review 2020

Selectie van statements ten behoeve van de peer-carrousel en de expert-review

Naam instelling	**MBO Instelling**
Naam medewerker	
E-mail	
Functie	

Datum audit	
Type audit	
Naam auditor	
Instelling	
E-mail	
Functie	

Nr.	ISO	Omschrijving	Benchmark 2019	Bevinding peer review	Beoordeelde bewijslast	Eventuele toelichting beoordeling	Akkoord
1.1	5.1.1	Beleidsregels voor informatiebeveiliging	3	Vastgesteld			
1.17	16.1.1	Verantwoordelijkheden en procedures.	3	Vastgesteld, mogelijk te laag beoordeeld			
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	3	Niet vastgesteld			
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	2				
3.5	11.1.3	Kantoren, ruimten en faciliteiten beveiligen	3				
4.5	12.3.1	Back-up van informatie	3				
4.8	12.6.1	Beheer van technische kwetsbaarheden	3				
4.13	16.1.5	Respons op informatiebeveiligingsincidenten	3				
5.18	9.4.3	Systeem voor wachtwoordbeheer	2				
P.5	privacy	Bewaartermijnen	2				

Niet vastgesteld
Vastgesteld
Vastgesteld, mogelijk te laag beoordeeld

- Scoreformulier: voor-ingevuld met scores
  - auditor vult in
  - vastgesteld / niet vastgesteld
  - beoordeelde bewijslast (inclusief de methode)
  - eventueel kan een (korte!) toelichting
  - akkoord mbo-instelling

Peer Review 2020

- Na het invullen verstuurt de auditor het formulier naar martijn.bijleveld@sambo-ict.nl, er is verder geen nazorg vereist.
- De uitslagen worden in de peer-review-rapportage geanonimiseerd.

NETWERK IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Het netwerkprogramma voor 12 maart:

Inhoud

5. Roept u maar!
6. Naar aanleiding van de Benchmark IBP/E mbo 2019
   - Werkgroep Tooling,
   - Werkgroep update toetsingskader,
   - Van 2.5 naar 3.0,
   - Peer Review
7. **Controle en logging, dat moet beter!**
   - Urgentie
   - Waar hebben we het over?
   - Uitstapje naar de ict-opleidingen.
   - SURF over cyberdreiging, Melvin Koelwijn, SURF

NETWERK IBP IN HET MBO

Kennisnet SURF saMBO-ICT

Inhoud

Monitoring en Logging……

Urgentie……

NETWERK IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Inhoud

Monitoring en Logging……Urgentie……

De 15 laagst scorende statements uit het IB-kader

1.19	18.1.3	Beschermen van registraties	2,1
6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers	2,1
1.5	6.1.5	Informatiebeveiliging in projectbeheer	2,0
4.14	17.1.2	Informatiebeveiligingscontinuïteit implementeren	2,0
6.7	15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	2,0
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	2,0
6.12	12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen	2,0
5.12	12.4.2	Beschermen van informatie in logbestanden	2,0
6.2	12.4.1	Gebeurtenissen registreren	2,0
4.19	17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	1,9
6.3	12.4.3	Logbestanden van beheerders en operators	1,8
6.9	18.2.2	Naleving van beveiligingsbeleid en –normen	1,8
2.8	6.2.2	Telewerken (thuiswerken)	1,7
5.27	14.3.1	Bescherming van testgegevens	1,7
6.11	7.2.1	Directieverantwoordelijkheden	1,5

NETWERK IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Inhoud

Monitoring en Logging……Urgentie……

De 15 laagst scorende statements uit het IB-kader

1.19	18.1.3	Beschermen van registraties	2,1
6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers	2,1
1.5	6.1.5	Informatiebeveiliging in projectbeheer	2,0
4.14	17.1.2	Informatiebeveiligingscontinuïteit implementeren	2,0
6.7	15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	2,0
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	2,0
6.12	12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen	2,0
5.12	12.4.2	Beschermen van informatie in logbestanden	2,0
6.2	12.4.1	Gebeurtenissen registreren	2,0
4.19	17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	1,9
6.3	12.4.3	Logbestanden van beheerders en operators	1,8
6.9	18.2.2	Naleving van beveiligingsbeleid en –normen	1,8
2.8	6.2.2	Telewerken (thuiswerken)	1,7
5.27	14.3.1	Bescherming van testgegevens	1,7
6.11	7.2.1	Directieverantwoordelijkheden	1,5

Inhoud

Monitoring en Logging…
waar hebben we het over?
Bijdrage van Co Klerkx, ROC van Amsterdam

IBP netwerkbijeenkomst
12-3-2020

- IBP monitoring & logging in de praktijk

Monitoring en logging

- Beleid monitoring & logging
- Protocol ICT medewerker
- Architectuur (applicatie, infrastructuur)
- Samenwerking ICT opleidingen (cyber security opleiding) en dienst ICT
- Samenwerking met Surf

Monitoring en logging

- **Beleid monitoring & logging**

7. Soorten logging

Logging ICT-voorzieningen kan in de volgende onderdelen worden verdeeld:

Categorie	Doel	Voor wie beschikbaar	Persoonsgegevens inzichtelijk ?	Systeem
Beschikbaarheid	Periodiek valideren of ICT componenten werken binnen de afgesproken kaders	Bepaalde functies binnen Dienst ICT	NEE, gegevens worden per tijdseenheid anoniem ingelezen	Solarwinds, SCCM
Diagnose	Incidenten oplossen (End-to-End view) Misbruik van techniek kunnen achterhalen (bijv. DDoS)	Bepaalde functies binnen Dienst ICT	JA, verkeersgegevens en locatiegegevens worden bijgehouden voor een beperkte periode	Prime, FortiAnalyzer
Archief	Ter ondersteuning van een redelijk vermoeden van onrechtmatig gebruik, dan wel misbruik van de ICT-infrastructuur	Specifiek benoemde beheerders en alleen na goedkeuring directie / bestuur	JA, verkeersgegevens en gebruikersnaam worden bijgehouden voor een langere periode	Nader te bepalen, per case

Monitoring en logging

- **Protocol ICT medewerker**

  Artikel 7

  De ICT-functionaris zal gericht onderzoek naar niet toegestaan gebruik van e-mail en / of informatie-systemen alleen na uitdrukkelijke en schriftelijke opdracht van de Raad van Bestuur of gemandateerde(n) uitvoeren.

  Artikel 12

  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 leiding-gevende. Bij mogelijke belangenverstrengeling kan melding worden gedaan bij de Functionaris Gegevensbescherming.

Monitoring en logging

- **Architectuur**

  - NOC: network operation center

  - SOC: security operation center

    (SIEM security information event management)

  - Architect security
  - ICT security specialist (nieuwe rol)

  - Uitdaging voor realisatie: beschikbaarheid en kennis

Monitoring en logging

- Samenwerking ICT opleidingen (cyber security opleiding) en dienst ICT, ondersteuning docenten.
- Samenwerking cybersecurity MBO-HBO-bedrijfsleven
- Cyber security vraagt HBO niveau

Monitoring en logging

- **Aandacht voor:**
- Samenwerking met SURF, saMBO-ICT
- SOC als SURFdienst?
- HOT item door ransomware UvM

NETWERK IBP IN HET MBO

Kennisnet SURF saMBO-ICT

Inhoud

Monitoring en Logging…
Hoe pakken ze dat bij SURF aan?
Presentatie van Melvin Koelewijn, SURFnet

NETWERK IBP IN HET MBO
Kennisnet SURF saMBO-ICT

Het netwerkprogramma voor 12 maart:

Inhoud

8. **In werkgroepen bespreken van het thema**
   - Hoe werkt dat bij jouw instelling, uitwisseling ervaringen
   - Welke knelpunten zie je, benoem de drie belangrijkste knelpunten
   - Stellingen: trek conclusies uit het besprokene, maak één stelling over monitoring en logging en stel een kort advies op voor de regiegroep m.b.t. monitoring en logging.
9. Terugkoppeling en adviezen vanuit de werkgroepen
10. Afronding, buffet, informeel netwerken.

Korte terugkoppeling en afronding. Borrel en buffet