Benchmark informatiebeveiliging en privacy in de mbo sector 2016

IBPDOC20

GEBRUIKERSGROEP IBP IN HET MBO

Kennisnet SURF saMBO-ICT

Verantwoording

Productie

Kennisnet / saMBO-ICT
Benchmark is uitgevoerd met behulp van de tool Coable van het bedrijf Coblue Sybersecurity.
Het Hoger Onderwijs (SURF SCIPR) maakt ook gebruik van deze tool.

Auteurs

Ludo Cuijpers	(Kennisnet, ROC Leeuwenborgh)
Rene Dol	(Deltion)
Esther van de Hei	(Nimeto)
December 2016	

Met dank aan

Aeres Groep	Martin Deiman
Albeda	Rienk de Vries
Arcus College	Joep Lemmens
Aventus	Fung-Yee Poon
Citaverde	Martijn van Hoorn
Clusius	Chris Houthuijs
Deltion	Rene Dol
Graafschap College	Paul Hoeken
Grafisch Lyceum Rotterdam	Don van der Linden
Helicon	Paul Kremers
Hoornbeeck	Willem Flink
Hout en Meubel College	Jan de Hooge
Lentiz	Rene Bosman
Koning Willem 1 College	Frits van Zadelhoff
MBO Utrecht	Marjolein Rombouts
Nimeto	Esther van der Hei
Noorderpoort	Martijn Broekhuizen
Nordwin College	Rob Smit
Nova College	Rob Smit
Onderwijsgroep Tilburg	Brom Bogers
ROC A12	Henk Links
ROC Leeuwenborgh	Nico Hermans
ROC Midden Nederland	Rene van der Mark
ROC Rijn Ijssel	Maarten Veldhuis
ROC TOP	Theo Kuilboer
ROC Twente	Kim Kuipers
ROC van Amsterdam	Co Klerkx
ROC West Brabant	Jan van den Hazelkamp
Summa College	Martien van Beekveld
Zadkine	Wim Arendse

Sommige rechten voorbehouden

Inhoudsopgave

1. Conclusies IBP benchmark 2016

1.1 Terugblik

Medio 2014 is de Taskforce Informatiebeveiliging en privacy van start gegaan met een duidelijke opdracht die verwoord is in het Verantwoordingsdocument[1]. De eerste paragraaf spreekt boekdelen:

> *… Het zal duidelijk zijn dat het thema Informatiebeveiliging en zeker ook privacy de laatste tijd met een sneltreinvaart in het onderwijs in de belangstelling is komen te staan. Dat heeft zo zijn redenen. Afgelopen jaren zijn in alle sectoren van het onderwijs incidenten rondom examinering in de publiciteit gekomen. In sommige gevallen ging dit ook om ernstige incidenten die breed in de media zijn uitgemeten. Dat levert voor het onderwijs veel schade op, waarbij imagoschade voorop staat. Het onderwijs wordt geacht op betrouwbare wijze diploma's uit te reiken en het kan niet zo zijn dat daar twijfels over bestaan omdat examens op straat liggen dan wel op het internet te koop zijn. Een ander voorbeeld is de vraag of het onderwijs met de toenemende registratie van gegevens van leerlingen de bescherming van de privacy nog kan waarborgen. Steeds vaker zijn hier ook externe partijen en leveranciers bij betrokken en zonder goede afspraken hierover kan de privacybescherming zomaar in het geding zijn. Zeker bij jonge kinderen wordt dit door de maatschappij onacceptabel gevonden.*
>
> ***Daar komt bij dat een vraag naar hoe het in de onderwijs sector gesteld is met de informatiebeveiliging en de bescherming van de privacy nauwelijks kan worden beantwoord. Dat beeld is op zijn minst zeer gebrekkig en onhelder te noemen. En om aan te geven of je iets op orde hebt moet je daarover ook eerste afspraken gemaakt hebben over wat dan op orde is. Die afspraken ontbreken vooralsnog.***
>
> *Daarom is het in het belang van zowel het onderwijs zelf als van het ministerie van Onderwijs, Cultuur en Wetenschap (OCW) dat er gemeenschappelijke afsprakenkaders komen, dat die met alle onderwijsinstellingen en ook met de relevante externe partijen worden gedeeld en geïmplementeerd. Pas dan kan er een beeld ontstaan van hoe scholen het doen op deze terreinen en kunnen er verbeteringstrajecten worden ingezet en doelen gesteld worden om een bepaalde graad van beveiliging en bescherming te creëren. In het hoger onderwijs is dit traject al eerder ingezet.*
>
> *Dit alles heeft er toe geleid dat OCW de vraag bij de mbo sector heeft neergelegd om een beeld van de stand van zaken in het mbo met betrekking tot informatiebeveiliging en privacy te schetsen en er voor te zorgen dat er naar een gewenste situatie kan worden toegewerkt. De sector heeft deze uitdaging opgepakt en wil met dit programma de stappen zetten om in het mbo op een volwassen wijze met deze problematiek om te gaan en een acceptabel niveau van beveiliging en bescherming te bieden aan al haar studenten en medewerkers….*

Als sector hebben we het afgelopen jaren hard gewerkt om Informatiebeveiliging en privacy in onze sector op de strategische agenda te zetten. Op tactisch niveau hebben we een groot aantal documenten opgeleverd (zie bijlage 1) en is er volop geschoold in de masterclasses informatiebeveiliging en privacy (ibp) waar een vijftigtal mbo instellingen aan hebben deelgenomen. Op operationeel niveau is deze kennis binnen de mbo instellingen vertaald in een actief IBP beleid. Weliswaar staan we als sector aan het begin van een lange weg maar toch hebben we het gevoel dat we een vliegende start hebben gemaakt. We willen nu graag voor het tweede achtereenvolgende jaar weten waar de mbo sector staat. Daarvoor hebben we wederom een benchmark uitgevoerd om de bepalen op welk volwassenheidsniveau we ons nu bevinden.

1.2 Representativiteit

Aan de eerste IBP benchmark (2015) hebben 19 mbo instellingen deel genomen waaronder 3 AOC's, 14 ROC's en 2 vakscholen. De regionale spreiding was afdoende. Zowel grote (ROC Amsterdam) als kleine (Nimeto) mbo instellingen hebben deelgenomen. Het is dan ook statistisch verdedigbaar dat deze deelwaarneming een getrouw beeld schetst van de 51 mbo instellingen die actief betrokken zijn bij het informatie en privacy beleid in onze sector. Van 14 instellingen was in 2015 niet duidelijk of zij stappen genomen hadden op dit gebied.

Aan de tweede benchmark (2016) hebben 30 mbo instellingen deelgenomen. Alle mbo instellingen hebben inmiddels stappen gezet op het gebied van informatiebeveiliging en privacy.

[1] Zie IBPDOC1: Verantwoordingsdocument Informatiebeveiliging en privacy (ibp) in het mbo.

1.3 Algemene bevindingen informatiebeveiliging

De benchmark is uitgevoerd op basis van het vastgestelde toetsingskader ibp[2]. De toets is dan ook uitgevoerd op de 6 clusters die afgeleid zijn van het ISO 27001/2 normenkader. De opzet van de benchmark is gelijk aan die van het Hoger Onderwijs.

Een samenvatting van de resultaten, de gemiddelde scores van alle mbo instellingen van alle statements (onderzochte onderwerpen) per cluster (tussen haakjes resultaat 2015):

Cluster 1: Beleid en organisatie	**1.8** (1.7)
Cluster 2: Personeel, studenten en gasten	**1.7** (1.7)
Cluster 3: Ruimtes en apparatuur	**2.2** (2.1)
Cluster 4: Continuïteit	**2.1** (2.0)
Cluster 5: Vertrouwelijkheid en integriteit	**2.0** (2.0)
Cluster 6: Controle en Logging	**1.6** (1.6)

De gemiddelde score van de mbo sector is: **1,9** (1,9)
Ter vergelijking de score van het Hoger Onderwijs in 2013 was 2,2.
In hoofdstuk 2 worden de resultaten verder toegelicht.

[2] IBPDOC3: Toetsingskader informatiebeveiliging cluster 1 t/m 6

1.4 Gedetailleerde bevindingen informatiebeveiliging

		1	2	3	4	5
		Allen 2016	Kern 2016	Kern 2015	Peer 2016	AOC's 2016
ISO27002	Statement	Gemiddeld	Gemiddeld	Gemiddeld	Gemiddeld	Gemiddeld
5.1.1.1	Beleidsregels voor informatiebeveiliging	2,2	2,5	1,8	2,2	2,3
	Cluster 1: Beleid en organisatie (2015: 1,7)	1,8	1,9	1,6	1,7	1,7
7.1.2	Arbeidsvoorwaarden	2,0	2,3	1,9	2,0	1,8
7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	1,4	1,6	1,3	1,4	1,2
	Cluster 2: Personeel, studenten en gasten (1,7)	1,7	1,9	1,6	1,7	1,6
	Cluster 3: Ruimtes en apparatuur (2015: 2,1)	2,2	2,1	2,0	2,0	1,9
12.1.2	Wijzigingsbeheer	2,3	2,5	2,2	2,4	2,3
17.1.2	Informatiebeveiligingscontinuïteit implementeren	1,4	1,6	1,4	1,4	1,2
	Cluster 4: Contnuïteit (2015: 2,0)	2,1	2,1	1,9	2,1	2,1
9.1.1	Beleid voor toegangsbeveiliging	2,2	2,3	2,1	2,1	2,0
9.1.2	Toegang tot netwerken en netwerkdiensten	2,3	2,4	2,3	2,2	2,2
9.2.1	Registratie en afmelden van gebruikers	2,3	2,3	2,3	2,4	2,3
	Cluster 5: Vertrouwelijkheid en integriteit (2,0)	2,0	2,1	1,9	2,0	2,0
9.2.5	Beoordeling van toegangsrechten van gebruikers	1,8	1,8	1,6	1,8	1,8
12.4.3	Logbestanden van beheerders en operators	1,6	1,6	1,5	1,6	1,5
18.2.2	Naleving van beveiligingsbeleid en –normen	1,5	1,7	1,4	1,5	1,5
	Cluster 6: Controle en logging (2015: 1,6)	1,6	1,7	1,5	1,6	1,5

Kolom 1 (**Allen 2016**): geeft de gemiddelde score weer van alle deelnemende mbo instellingen.

Kolom 2 (**Kern 2016)**: geeft de score weer van de 12 instellingen die zowel in 2016 als in 2015 deelnamen aan de benchmark.
Opvallend is dat ze hoger scoren dan “Allen 2016”. Het statement “Beleidsregels voor informatiebeveiliging” scoort bovengemiddeld (2,5).

Kolom 3 **(Kern 2015**): geeft de score weer van de 12 instellingen die zowel in 2016 als in 2015 deelnamen aan de benchmark.
Opvallend is dat de score van 2015 flink verbeterd is in 2016 (Kolom 2 (**Kern 2016)**).

Kolom 4 **(Peer 2016**): geeft de score weer van de 16 instellingen die in 2016 hebben deelgenomen aan de Peer Review.
De score wijkt amper af van het gemiddelde “Allen 2016”.

Kolom 5 **(AOC’s 2016**): geeft de score weer van de 6 AOC’s die hebben deelgenomen aan de benchmark.
De score wijkt amper af van het gemiddelde “Allen 2016”.

1.5 Benchmark privacy

De gemiddelde score van de benchmark privacy bedraagt 1,5. Dit is teleurstellend in de wetenschap dat de sector over ruim 1 jaar (25 mei 2018, ingangsdatum AVG) een score 3 zou moeten kunnen halen. De rood gearceerde statements scoren te laag. Een score 1,1 of 1,2 geeft aan dat er binnen de sector maar een handvol mbo instellingen beleid op dit statement hebben ontwikkeld. Aan deze benchmark hebben 20 mbo instellingen deel genomen.

1.5.1 Beleid en organisatie

Nr.	Statement	Beoordeling
P.1	Privacy-beleid	1,9
P.2	Functionaris gegevensbescherming	1,9
P.3	Doelbepaling, doelbinding, grondslag, grond bij minderjarigen en dataminimalisatie	1,3
P.4	Registratieplicht	1,1
P.5	Bewaartermijnen	1,4
P.6	Verwerking t.b.v. onderzoek	1,2
P.7	Verwerking van bijzondere persoonsgegevens	1,4
P.8	Geautomatiseerde besluitvorming	1,2
P.9	Informatiebeveiliging	1,8
P.10	Bewerkersovereenkomsten	2,0

1.5.2 Personeel, studenten en gasten

Nr.	Statement	Beoordeling
P.11	Transparantie privacy beleid	1,8
P.12	Informatieplicht verwerkingen	1,4
P.13	Rechten van betrokkene	1,6
P.14	Arbeidsvoorwaarden	1,9
P.15	Bewustzijn, opleiding en training ten aanzien van privacy	1,2

1.5.3 Ruimtes en apparatuur

Nr.	Statement	Beoordeling
P.16	Verwijderen van persoonsgegevens	1,9

1.5.4 Vertrouwelijkheid en integriteit

Nr.	Statement	Beoordeling
P.17	Datakwaliteit (data-integriteit)	1,9
P.18	Datalek	1,8
P.19	Bijzondere persoonsgegevens	1,7

1.5.5 Controle en logging

Nr.	Statement	Beoordeling
P.20	Privacy in informatiesystemen	1,2
P.21	Gegevensbeschermingseffectbeoordeling (GEB, voorheen PIA)	1,1
P.22	Naleving van privacy beleid en –normen	1,4
P.23	Rapportage van privacy-gebeurtenissen	1,6
P.24	Gebeurtenissen registreren	1,5

1.6 Aanbevelingen

Op basis van de benchmark komen de 30 deelnemende mbo instellingen tot de volgende aanbevelingen:

- Vertaling beleid naar concrete maatregelen en hulpmiddelen
  Voorbeelden: Digitale awareness training, Encrypted email voor decanen, Encryptie van mobiele devices
- Vertaalslag van beleid naar concrete dingen: practices uitwisselen!
- Training voor proceseigenaren organiseren?
- Wat doe je bij incidenten? Incidenten delen en wat heb je dan gedaan?
- Register van Persoonsgegevens (AVG) (P4 uit het toetsingskader Privacy): hoe gedetailleerd moet die zijn? Zijn er sets te maken die breed te delen, inclusief maatregelen? Kunnen we hier gezamenlijk iets mee te doen?
- Masterclass (inleiding) Functionaris Gegevensbescherming (Registerplicht, Privacy risico, Best practice, etc.)
- Opleveren bewerkersovereenkomsten voor de 10 meest gebruikte applicaties in de mbo sector.
- Herschrijven toetsingskader naar nieuwe ontwikkelingen.
- Masterclass Privacy vanuit de praktijk.
- Overzicht beveiligingsklassen bewerkersovereenkomsten (Wim Konings).
- De afgelopen maanden heb ik verschillende verzoeken langs zien komen om gegevens te versturen naar externe partijen. Zo hebben we de JOB Monitor, Cultureel Jongeren Pas, MBO Studentenpas, gegevens naar basisscholen t.b.v. warme overdracht, etc… In veel (bijna alle) gevallen moeten we toestemming hebben van de leerling/ouder om deze gegevens te mogen versturen. Hoe kunnen we ervoor zorgen dat we de toestemming voor deze partijen op een makkelijke, maar legitieme manier kunnen regelen? We willen de leerling/ouder niet overladen met goedkeuringsformulieren. Wat is jullie advies om dit goed aan te pakken? (Niek Bunskoek).
- Een aanbeveling zou van mij s om classificeren en labelen extra aandacht te geven. Wordt laag op gescoord en blijkt voor meerdere organisaties lastig om dit praktisch in te vullen (Co Klerkx).
- Het onderwerp ‘bewerkersovereenkomsten’ bij ons is een aandachtspunt met hoge prioriteit; landelijke samenwerking en kennisdeling zou zeer gewenst zijn (Martijn van Hoorn).
- Maak een sjabloon **Register voor de verwerkingsactiviteiten** (Bram Bogers).
  De te beantwoorden vragen luiden: (Job Vos)
  - Wie is/zijn de verantwoordelijke(n) voor de gegevensverwerking?
  - Wat is het doel van de gegevensverwerking?
  - Van welke (categorieën) personen worden gegevens verwerkt?
  - Welke (categorieën) gegevens worden verwerkt?
  - Wie ontvangen gegevens uit de verwerking?
  - Hoe lang worden gegevens bewaard?
  - Worden persoonsgegevens doorgegeven naar landen buiten de Europese Unie?
  - Moet de Autoriteit Persoonsgegevens een voorafgaand onderzoek instellen naar de verwerking (lees: in geval van verwerking van een persoonsnummer voor een ander doel, verwerken persoonsgegevens uit heimelijke observatie, en strafrechtelijke gegevens verwerken)?

2. Resultaten ibp benchmark

2.1 Toelichting op de tabellen

Alle tabellen zijn op dezelfde manier opgebouwd. Een korte toelichting:

Nr.	ISO27002	Statement	2016	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5	2015
1.1	5.1.1.1	**Beleidsregels voor informatiebeveiliging**	2,2	6	13	10	1		1,9

Kolom 1, Nr. Geeft het nummer van het statement weer. Deze nummering is gelijk aan de nummering van het Hoger Onderwijs / MBO normenkader. Het eerste cijfer staat voor het cluster, het tweede cijfer voor het statement nummer.

Kolom 2. ISO27002 Geeft het nummer van de norm uit ISO27002. Een zestal normen zijn gesplitst in 12 statements. Dus 79 normen uit het ISO normenkader zijn gekoppeld aan 85 statements uit het HO/MBO normenkader.

		Clusterindeling Hoger Onderwijs						
Hoofdstukken ISO-27002	ISO-27002	**1**: Beleid	**2**: personeel	**3**: Ruimten	**4**: Continuïteit	**5**: Toegang	**6**: Controle	Niet gebruikt
5. Informatiebeveiligingsbeleid	**2**	2						
6. Organiseren van informatiebeveiliging	**7**	4		0				3
7. Veilig personeel	**6**		3					3
8. Beheer van bedrijfsmiddelen	**10**	2		1				7
9. Toegangsbeveiliging	**14**		1			9	1	3
10. Cryptografie	**2**	1				1		
11. Fysieke beveiliging en beveiliging van de omgeving	**15**	1	1	12				1
12. Beveiliging bedrijfsvoering	**14**			1	7	1	2	3
13. Communicatiebeveiliging	**7**	2	1			4		
14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen	**13**	1			1	1	3	7
15. Leveranciersrelaties	**5**	2			1		1	1
16. Beheer van informatiebeveiligingsincidenten	**7**	2	1		2		1	1
17. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	**4**				2			2
18. Naleving	**8**	2					2	4
	114	**19**	**7**	**14**	**13**	**16**	**10**	**35**
Clustertotaal inclusief splitsing (85)		21	7	15	15	17	10	

Nr.	ISO27002	Statement	2016	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5	2015
1.1	5.1.1.1	**Beleidsregels voor informatiebeveiliging**	**2,2**	**6**	**13**	**10**	**1**		1,9

Niveau 1, 2, 3, 4 en 5 verwijzen naar de volwassenheidsniveaus (maturity levels).

Het Normenkader informatiebeveiliging mbo wordt gebruikt om de volwassenheid van informatiebeveiliging te meten bij de mbo instellingen. Hiervoor wordt een 5-punts schaal gehanteerd gebaseerd op het Capability Maturity Model (CMM). Het CMM model is gebaseerd op procesvolwassenheid, de 5 niveaus zijn in de onderstaande tabel weergegeven.

CMM niveau	Omschrijving
niveau **1**	Initieel, ad hoc: De processen zijn ad hoc georganiseerd, erg afhankelijk van individuele personen **Ad hoc**
niveau **2**	Herhaalbaar, maar intuïtief: Er wordt op een vaste manier gewerkt **Beleid is gemaakt en goedgekeurd en bij een kleine groep bekend (opzet en bestaan).**
niveau **3**	Gedefinieerd proces: De processen zijn gedocumenteerd en bekend bij betrokkenen **Beleid is bij alle betrokken medewerkers, studenten en externen bekend (werking).**
niveau **4**	Beheerd en meetbaar: De processen worden beheerd, zitten in een verbetercyclus en zijn meetbaar (PDCA). **IBP is onderdeel geworden van de PDCA cyclus.**
Niveau **5**	Geoptimaliseerd: Er wordt als vanzelfsprekend verbeterd en volgens best practices gewerkt. **IBP is toekomstbestendig, effectief en efficiënt.**

Bij ieder volwassenheidsniveau is de score weergegeven van de deelnemende mbo instellingen aan de benchmark.
“Niveau 2” is rood omkaderd als een mogelijke baseline voor de sector.
De modale klasse (klasse met de hoogste frequentie dichtheid) is weergegeven in geel. Indien 2 klassen dezelfde dichtheid hebben is de hoogste klasse geel gearceerd. Grijs gearceerd geeft de modale klasse aan uit 2015 indien deze afwijkt van 2016.
Het gemiddelde cijfer (2016 en 2015) is het rekenkundige gemiddelde van de individuele waarnemingen.

2.2 Wat gaat goed en wat gaat minder goed?

Best scorende statements uit alle clusters.

Nr.	ISO27002	Statement	2016	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5	2015
4.5	12.3.1.1	Back-up van informatie	2,9	1	7	16	6		2,6
4.3	12.2.1.1	Beheersmaatregelen tegen malware	2,6		13	17			2,4
3.10	11.2.2	Nutsvoorzieningen	2,5	5	9	12	4		2,5
4.7	12.5.1	Software installeren op operationele systemen	2,5	3	12	13	2		2,5
4.9	12.6.2	Beperkingen voor het installeren van software	2,5	3	11	15	1		2,5
5.13	13.1.1	Beheersmaatregelen voor netwerken	2,5	2	12	15	1		2,5
3.12	11.2.4	Onderhoud van apparatuur	2,4		18	11	1		2,3
3.15	12.4.4	Kloksynchronisatie	2,4	4	12	13	1		2,1
5.9	9.4.2	Beveiligde inlogprocedures	2,4	1	16	13			2,3

Opvallend is dat de top 8 van de goed scorende statements allemaal in de cluster 3, 4 en 5 zitten. Technisch lijkt het dus in orde te zijn.

Slechts scorende statements uit alle clusters.

Nr.	ISO27002	Statement	2016	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5	2015
1.7	8.2.1	Classificatie van informatie	1,4	20	8	2			1,3
1.10	10.1.1.2	Beleid inzake het gebruik van cryptografische beheersmaatregelen	1,4	19	10	1			1,3
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	1,4	20	8	2			1,4
4.14	17.1.2	Informatiebeveiligingscontinuïteit implementeren	1,4	20	9	1			1,4
5.10	10.1.2.1	Sleutelbeheer	1,4	17	13				1,3
6.5	14.2.8	Testen van systeembeveiliging	1,4	20	9		1		1,3

Cluster 3 kent geen statement dat zeer slecht scoort. Cluster 1, beleid, komt tweemaal voor.

2.3 Beleid en organisatie

Nr.	ISO27002	Statement	2016	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5	2015
1.1	5.1.1.1	Beleidsregels voor informatiebeveiliging	2,2	6	13	10	1		1,9
1.2	5.1.1.2	Beleidsregels voor informatiebeveiliging (gecommuniceerd)	1,6	16	11	3			1,5
1.3	5.1.2	Beoordeling van het Informatiebeveiligingsbeleid	1,7	15	12	1	2		1,7
1.4	6.1.1	Taken en verantwoordelijkheden informatiebeveiliging:	2,2	6	13	11			2,1
1.5	6.1.5	Informatiebeveiliging in projectbeheer	1,6	15	13	2			1,5
1.6	6.2.1.1	Beleid voor mobiele apparatuur:	1,9	11	12	7			1,8
1.7	8.2.1	Classificatie van informatie	1,4	20	8	2			1,3
1.8	8.2.2	Informatie labelen	1,5	16	13	1			1,3
1.9	10.1.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	1,5	18	9	3			1,5
1.10	10.1.1.2	Beleid inzake het gebruik van cryptografische beheersmaatregelen	1,4	19	10	1			1,3
1.11	11.2.5	Verwijdering van bedrijfsmiddelen	1,8	12	11	7			1,7
1.12	13.2.1	Beleid en procedures voor informatietransport:	1,6	12	18				1,6
1.13	13.2.2	Overeenkomsten over informatietransport	1,8	10	15	5			1,9
1.14	14.1.1	Analyse en specificatie van informatiebeveiligingseisen	1,9	7	18	5			1,9
1.15	15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	1,8	11	14	5			1,5
1.16	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	1,9	8	17	5			1,7
1.17	16.1.1	Verantwoordelijkheden en procedures.	2,0	7	17	4	2		1,8
1.18	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	2,1	8	13	7	2		1,9
1.19	18.1.3	Beschermen van registraties	1,7	11	17	2			1,6
1.20	18.1.4	Privacy en bescherming van persoonsgegevens	2,0	4	23	3			1,9
1.21	6.1.2	Scheiding van taken	2,0	5	20	5			1,9
		Gemiddeld (2015: 1,7)	1,8						

In dit cluster valt veel winst te behalen. Een goedgekeurd ibp beleidsplan heeft invloed op de statements: 1.1, 1.2, 1.3, 1.4, 1.7, 1.8 en 1.20. Dit cluster is voor een gemiddelde instelling te behalen in een aantal maanden.

2.4 Personeel, studenten en gasten

Nr.	ISO27002	Statement	2016	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5	2015
2.1	7.1.2	Arbeidsvoorwaarden	2,0	9	13	8			1,9
2.2	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	1,4	20	8	2			1,4
2.3	9.2.6	Toegangsrechten intrekken of aanpassen	2,3	1	20	9			2,1
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	1,6	17	9	4			1,5
2.5	13.2.4	Vertrouwelijkheids- of geheimhoudingsovereen-komst	1,6	13	16	1			1,4
2.6	16.1.3	Rapportage van zwakke plekken in de informatie-beveiliging	1,5	15	15				1,4
2.7	7.1.1	Screening	1,8	12	13	4	1		2,1
		Gemiddeld (2015: 1,7)	1,7						

Dit is een moeilijk te realiseren cluster voor veel mbo instellingen. Met name de statements 2.2. en 2.4 vragen veel tijd en energie van alle medewerkers en studenten.

2.5 Ruimtes en apparatuur

Nr.	ISO27002	Statement	Gemid-deld	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5	2015
3.1	6.1.2.1	Beleid voor mobiele apparatuur	2,1	8	12	10			2,2
3.2	8.3.2	Verwijderen van media	2,0	7	16	6	1		2,0
3.3	11.1.1	Fysieke beveiligingszone	2,2	4	15	11			2,2
3.4	11.1.2	Fysieke toegangsbeveiliging	2,0	6	18	6			1,9
3.5	11.1.3	Kantoren, ruimten en faciliteiten beveiligen	2,0	6	17	7			2,1
3.6	11.1.4	Beschermen tegen bedreigingen van buitenaf	2,3	1	19	9	1		2,3
3.7	11.1.5	Werken in beveiligde gebieden	2,0	5	21	4			1,7
3.8	11.1.6	Laad- en loslocatie	1,9	12	12	4	2		1,9
3.9	11.2.1	Plaatsing en bescherming van apparatuur	2,3	2	18	8	2		2,5
3.10	11.2.2	Nutsvoorzieningen	2,5	5	9	12	4		2,5
3.11	11.2.3	Beveiliging van bekabeling	2,3	5	12	11	2		2,2
3.12	11.2.4	Onderhoud van apparatuur	2,4		18	11	1		2,3
3.13	11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	1,9	8	18	4			1,8
3.14	11.2.7	Veilig verwijderen of hergebruiken van apparatuur	1,9	7	18	5			2,1
3.15	12.4.4	Kloksynchronisatie	2,4	4	12	13	1		2,1
		Gemiddeld (2015: 2,1)	2,2						

Het best scorende statement van de mbo sector; geeft weinig aanleiding voor kritische beschouwingen. Feit blijft dat een aantal instellingen dit niveau niet realiseren. Nader onderzoek is dan ook gewenst om de oorzaak te kunnen achterhalen.

2.6 Continuïteit

Nr.	ISO27002	Statement	2016	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5	2015
4.1	12.1.2	Wijzigingsbeheer	2,3	4	14	11	1		2,2
4.2	12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen	2,2	4	18	7	1		1,9
4.3	12.2.1.1	Beheersmaatregelen tegen malware	2,6		13	17			2,4
4.4	12.2.1.2	Beheersmaatregelen tegen malware	1,8	12	11	7			1,8
4.5	12.3.1.1	Back-up van informatie	2,9	1	7	16	6		2,6
4.6	12.3.1.2	Back-up van informatie	2,2	5	16	7	2		2,0
4.7	12.5.1	Software installeren op operationele systemen	2,5	3	12	13	2		2,5
4.8	12.6.1	Beheer van technische kwetsbaarheden	1,7	11	17	2			1,8
4.9	12.6.2	Beperkingen voor het installeren van software	2,5	3	11	15	1		2,5
4.10	14.2.6	Beveiligde ontwikkelomgeving	1,9	8	18	4			1,7
4.11	15.2.2	Beheer van veranderingen in dienstverlening van leveranciers	1,8	8	20	1	1		1,7
4.12	16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	1,8	10	16	4			1,6
4.13	16.1.5	Respons op informatiebeveiligingsincidenten	2,0	8	16	5	1		1,7
4.14	17.1.2	Informatiebeveiligingscontinuïteit implementeren	1,4	20	9	1			1,4
4.15	17.2.1	Beschikbaarheid van informatie verwerkende faciliteiten	1,8	11	15	3	1		1,8
		Gemiddeld (2015: 2,0)	2,1						

Cluster 4 scoort goed. Opvallend is statement 4,14 dat uit de toon valt. Nota bene een belangrijk statement in het ibp veld (informatiebeveiligingscontinuïteit implementeren).

2.7 Vertrouwelijkheid en integriteit

Nr.	ISO27002	Statement	2016	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5	2015
5.1	9.1.1	Beleid voor toegangsbeveiliging	2,2	1	23	5	1		2,2
5.2	9.1.2	Toegang tot netwerken en netwerkdiensten	2,3	3	17	9	1		2,3
5.3	9.2.1	Registratie en afmelden van gebruikers	2,3	2	17	10	1		2,4
5.4	9.2.2	Gebruikers toegang verlenen	2,0	4	22	4			1,9
5.5	9.2.3	Beheren van speciale toegangsrechten	2,1	1	25	4			2,0
5.6	9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	2,1	6	14	10			2,2
5.7	9.3.1	Geheime authenticatie-informatie gebruiken	1,9	12	9	8	1		2,0
5.8	9.4.1	Beperking toegang tot informatie	2,2	3	17	10			2,2
5.9	9.4.2	Beveiligde inlogprocedures	2,4	1	16	13			2,3
5.10	10.1.2.1	Sleutelbeheer	1,4	17	13				1,3
5.11	10.1.2.2	Sleutelbeheer	1,5	18	11		1		1,3
5.12	12.4.2	Beschermen van informatie in logbestanden	1,6	14	14	1	1		1,6
5.13	13.1.1	Beheersmaatregelen voor netwerken	2,5	2	12	15	1		2,5
5.14	13.1.2	Beveiliging van netwerkdiensten	2,0	10	11	9			1,8
5.15	13.1.3	Scheiding in netwerken	2,3	5	10	15			2,2
5.16	13.2.3	Elektronische berichten	1,9	8	18	4			1,8
5.17	14.1.3	Transacties van toepassingen beschermen	1,6	16	11	3			1,6
		Gemiddeld (2015: 2,0)	2,0						

Dit cluster scoort gemiddeld. Opvallend is dat het (digitaal) sleutelbeheer (encryptie) onder de maat scoort.

2.8 Controle en Logging

Nr.	ISO27002	Statement	2016	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5	2015
6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers	1,8	10	17	3			1,7
6.2	12.4.1	Gebeurtenissen registreren	1,7	11	17	2			1,6
6.3	12.4.3	Logbestanden van beheerders en operators	1,6	14	15	1			1,6
6.4	14.2.7	Uitbestede softwareontwikkeling	1,6	13	16	1			1,6
6.5	14.2.8	Testen van systeembeveiliging	1,4	20	9		1		1,3
6.6	14.2.9	Systeemacceptatietests	2,0	8	15	6	1		2,0
6.7	15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	1,6	14	15	1			1,5
6.8	16.1.7	Verzamelen van bewijsmateriaal	1,5	16	13		1		1,4
6.9	18.2.2	Naleving van beveiligingsbeleid en –normen	1,5	14	16				1,5
6.10	18.2.3	Beoordeling van technische naleving	1,5	16	12	2			1,5
		Gemiddeld (2015: 1,6)	1,6						

Dit cluster scoort ver onder de maat. Registratie van informatie zal sector breed aangepakt moeten worden.

3. Benchmark compliance-kader: Privacy

3.1 Beleid en organisatie

Nr.	Statement	Beoordeling
P.1	**Privacy-beleid**: Ten behoeve van het garanderen van privacy van deelnemers en medewerkers en om te voldoen aan de relevante wet- en regelgeving, behoort een reeks beleidsregels te worden gedefinieerd en goedgekeurd door het bestuur. In dit beleid is voorzien in procedures voor het uitoefenen van de rechten van deelnemers en docenten.	1,9
P.2	**Functionaris gegevensbescherming:** De instelling benoemt een functionaris voor de gegevensbescherming (FG), of indien dit niet mogelijk of wenselijk is een privacy officer (PO), die is belast met intern toezicht op de verwerkingen van persoonsgegevens binnen de instelling, en alle verwerkingen van persoonsgegevens inventariseert en registreert. De verantwoordelijke zorgt er voor dat alle andere beroepswerkzaamheden van de FG verenigbaar zijn met zijn taken en verplichtingen als FG en dat die niet tot een belangenconflict leiden.	1,9
P.3	**Doelbepaling, doelbinding, grondslag, grond bij minderjarigen, dataminimalisatie.** De instelling draagt er zorg voor dat de deze zaken zijn vastgesteld.	1,3
P.4	**Registratieplicht:** Een verwerking van persoonsgegevens wordt gemeld aan de aangestelde Functionaris Gegevensbescherming die daartoe een (openbaar) register bijhoudt.	1,1
P.5	**Bewaartermijnen:** Er is een actief archief- en vernietigingsbeleid: persoonsgegevens worden niet langer bewaard dan nodig voor het gestelde doeleinde. De instelling stelt op basis van de Archiefwet de vernietigings- en bewaartermijnen vast van de verwerkte persoonsgegevens. De instelling is in staat om *alle* persoonsgegevens die niet onder een wettelijke bewaartermijn vallen, op een eerste verzoek van de deelnemer (of als deze jonger is dan 16 jaar: diens ouders) te vernietigen.	1,4
P.6	**Verwerking t.b.v. onderzoek:** Persoonsgegevens mogen worden verwerkt ten behoeve van: archivering in het algemeen belang (Archiefwet); wetenschappelijk of historisch onderzoek of statistische doeleinden.	1,2
P.7	**Verwerking van bijzondere persoonsgegevens:** De instelling verwerkt geen persoonsgegevens betreffende • iemands religieuze of levensbeschouwelijke overtuigingen, • ras of etnische afkomst, • biometrische gegevens (zoals vingerafdruk of irisscan) met het oog op de unieke identificatie van een persoon, • gezondheid of iemands seksueel gedrag of seksuele gerichtheid	1,4

P.8	**Geautomatiseerde besluitvorming:**
	In geval de instelling gebruik maakt van geautomatiseerde individuele besluitvorming:
	• zal de onderwijsinstelling geen geautomatiseerde beslissingen laten nemen over de betrokkene zonder dat bij die beslissing een natuurlijk persoon namens de instelling betrokken is, tenzij de betrokkene instemt met een geautomatiseerde beslissing zonder menselijke interventie; en
	• zal er aan de betrokkene duidelijke informatie worden verstrekt over de wijze van profilering, en
	• heeft de betrokkene de mogelijkheid
	  • zijn standpunt en visie over het besluit en besluitvormingsproces te geven, en
	  • in verweer te komen tegen een dergelijke geautomatiseerde beslissing; en
	  • worden er bij de besluitvorming geen bijzondere persoonsgegevens gebruikt.
		1,2

P.9	**Informatiebeveiliging**: De instelling neemt passende technische of organisatorische maatregelen op een dusdanige manier dat de passende beveiliging van persoonsgegevens gewaarborgd is. De integriteit en vertrouwelijkheid van de persoonsgegevens moet gegarandeerd zijn. Verwerkte persoonsgegevens zijn beveiligd tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze beveiliging is afhankelijk van de stand van de techniek, de uitvoeringskosten, alsook de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de privacy van de onderwijsdeelnemers. Bij de beveiliging wordt aangesloten bij algemeen geaccepteerde beveiligingsstandaarden binnen de praktijk van de informatiebeveiliging.	1,8
P.10	**Bewerkersovereenkomsten**: Met alle leveranciers die als bewerker voor of namens de instelling persoonsgegevens (van deelnemers, medewerkers en externen) verwerken, worden bewerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld.	2,0

3.2 Personeel, studenten en gasten

Nr.	Statement	Beoordeling
P.11	**Transparantie privacy beleid:** De instelling informeert de (ouders van) deelnemers en medewerkers van wie persoonsgegevens worden verwerkt, beknopt, transparant, eenvoudig toegankelijk en begrijpelijk in duidelijke en eenvoudige taal over het privacy beleid en de rechten en verplichtingen van betrokkenen.	1,8
P.12	**Informatieplicht verwerkingen:** De instelling informeert actief, al dan niet met gebruikmaking van door leveranciers geleverde informatie, aan de (ouders van) deelnemers en medewerkers van wie persoonsgegevens worden verwerkt, welke verwerking er in welke informatiesystemen binnen de instelling plaatsvindt en welke maatregelen er zijn getroffen om de privacy van die deelnemer te kunnen waarborgen. Aan de betrokken deelnemers en docenten wordt beknopt, transparant, eenvoudig toegankelijk en begrijpelijk in duidelijke en eenvoudige taal ten minste medegedeeld: • De identiteit en contactgegevens van de verantwoordelijke (CvB van de onderwijsinstelling), • De contactgegevens van de FG of PO, • welke (categorieën) persoonsgegevens worden verwerkt, • het doel van de verwerking, • of die verwerking beperkt is tot dat wat voor het gestelde doeleinde strikt noodzakelijk is, • of persoonsgegevens ook voor andere doeleinden worden verwerkt, • wat de bewaar- en vernietigingstermijnen zijn; • of persoonsgegevens worden gedeeld met commerciële derden, • of persoonsgegevens worden verkocht of verhuurd, • of persoonsgegevens gecodeerd worden bewaard.	1,4
P.13	**Rechten van betrokkene:** De instelling respecteert expliciet de volgende rechten: **P.13.a.** Deelnemers (dan wel hun ouders) en medewerkers hebben het recht een verzoek te doen ter verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens, in het geval dat deze gegevens: • feitelijk onjuist zijn, • voor het gestelde doeleinde onvolledig of niet ter zake dienend zijn, • de verwerking van de persoonsgegevens niet meer nodig is, • dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. **P.13.b.** De verbetering, aanvulling of verwijdering wordt voor zover redelijkerwijs mogelijk doorgegeven aan alle personen en organisaties die van de onderwijsinstelling hebben ontvangen. **P.13.c.** Deelnemers hebben het recht om geheel 'te worden vergeten' door het verwijderen van alle persoonsgegevens, tenzij de onderwijsinstelling op grond van een wettelijke plicht, of ter vrijwaring van een rechtsvordering deze gegevens moet bewaren. Evenmin worden de gegevens verwijderd indien deze verwijdering een inbreuk op vrijheid van meningsuiting en informatie oplevert. **P.13.d.** In geval de verwerking van persoonsgegevens plaatsvindt op basis van toestemming of een overeenkomst, heeft de deelnemer heeft recht om de door de onderwijsinstelling verwerkte persoonsgegevens in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen. **P.13.e.** De betrokken deelnemer wordt in kennis gesteld van de door de onderwijsinstelling uitgevoerde handelingen met zijn persoonsgegevens.	1,6
P.14	**Arbeidsvoorwaarden**: In de contractuele overeenkomst met medewerkers en contractanten zijn hun (eventuele) verantwoordelijkheden voor privacy opgenomen. In deze overeenkomst is voorzien in een vertrouwelijkheids- of geheimhoudingsbeding ten aanzien van de verwerkte persoonsgegevens.	1,9
P.15	**Bewustzijn, opleiding en training ten aanzien van privacy:** Alle interne en externe medewerkers van de organisatie behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie. De FG is hierbij betrokken.	1,2

3.3 Ruimtes en apparatuur

Nr.	Statement	Beoordeling
P.16	**Verwijderen van persoonsgegevens:** Van apparatuur die niet langer wordt gebruikt, worden de op het apparaat aanwezige persoonsgegeven op een betrouwbare en veilige wijze vernietigd. Vernietiging is mogelijk door vernietiging van de gegevensdrager zelf. In geval van vernietiging door een derde, geeft deze een verklaring af aangaande vernietiging.	1,9

3.4 Vertrouwelijkheid en integriteit

Nr.	Statement	Beoordeling
P.17	**Datakwaliteit (data-integriteit):** De verantwoordelijke gaat zorgvuldig om met de verwerkte persoonsgegevens en waarborgt het behoud en bescherming van de juistheid en de consistentie van die gegevens.	1,9
P.18	**Datalek:** In geval van een inbreuk in verband met de (beveiliging van) persoonsgegevens die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens. En die inbreuk houdt een risico in voor de rechten en vrijheden van betrokkenen, dan meldt de verantwoordelijke de inbreuk bij de AP zo snel mogelijk, doch uiterlijk binnen 72 uur nadat de inbreuk bekend is geworden. Deze inbreuk wordt aan getroffen betrokkenen gemeld indien de inbreuk een waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen. De getroffen deelnemers en medewerkers worden geïnformeerd over de aard van de inbreuk, en de gevolgen van de inbreuk op hun privacy.	1,8
P.19	**Bijzondere persoonsgegevens:** Bij verwerking van bijzondere persoonsgegevens zoals gezondheidsgegevens, neemt de instelling (extra) passende, consequente en specifieke maatregelen om de veiligheid van de gegevens te garanderen. Het gebruik van deze bijzondere gegevens blijft beperkt tot alleen die gevallen dat de informatie strikt noodzakelijk en evenredig is.	1,7

3.5 Controle en logging

Nr.	Statement	Beoordeling
P.20	Privacy in informatiesystemen: Bij het gebruiken en/of ontwerpen van informatiesystemen die persoonsgegevens van deelnemers en medewerkers verwerken, worden privacyregels zoals privacy by design en privacy by default in die systemen een aangehouden en zo mogelijk ingebouwd: • Gegevensminimalisatie af te dwingen (zo min mogelijk vrije velden) • Transparantie over gebruik van gegevens • Afschermen van de identiteit (pseudonimisering) • Gebruik sticky policies • Data tracking (waaronder logging).	1,2

P.21	**Gegevensbeschermingseffectbeoordeling (GEB, voorheen PIA):**
	• De instelling voert een (tweejaarlijks terugkerende) evaluatie uit van de mogelijke effecten van de verschillende gegevensverwerking op de rechten en vrijheden van de betrokkenen. Deze evaluatie vindt eveneens plaats in geval van een wijziging in de verwerking van persoonsgegevens die specifiek de risico's wijzigt voor de privacy van de betrokken deelnemers en medewerkers.
	• De instelling voert naar aanleiding van de evaluatie een volledige GEB uit in geval de verwerking van de persoonsgegevens:
	  • in geval van een systematische en uitgebreide beoordeling van persoonlijke aspecten van betrokkenen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;
	  • Bijzondere persoonsgegevens (ras, gezondheid) worden verwerkt;
	  • Geautomatiseerde bewaking van publiek toegankelijke ruimtes.
	• De beoordeling heeft betrekking op de gehele levenscyclus van persoonsgegevens van verzameling van verwerking tot verwijdering.
	• In geval van herziening van of nieuwe verwerkingen van grote hoeveelheden persoonsgegevens, wordt vooraf bepaald wat de impact is van deze (gewijzigde) verwerking op de privacy van de deelnemers.
	Bij de GEB is altijd de FG betrokken.
		1,1

P.22	**Naleving van privacy beleid en –normen:** De instelling controleert (laat controleren) regelmatig de naleving van de privacy regels en informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging. De FG ziet toe op de (dagelijkse) naleving van het beleid.	1,4
P.23	**Rapportage van privacy-gebeurtenissen**: Privacy- en informatiebeveiligingsincidenten behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd aan de FG en verantwoordelijke.	1,6
P.24	**Gebeurtenissen registreren:** Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig beoordeeld.	1,5

Bijlage 1: Framework informatiebeveiliging en privacy in het mbo