**Benchmark informatiebeveiliging en privacy in de mbo sector 2017**

****

**IBPDOC11c**

**Verantwoording**

**Productie**

Kennisnet / saMBO-ICT

**Auteurs**

Leo Bakker (Kennisnet)

Ludo Cuijpers (Kennisnet, ROC Leeuwenborgh)

December 2017

**Met dank aan**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | Martijn Deiman | Aeres Groep | 25 | Bram Bogers | Onderwijsgroep Tilburg |
| 2 | Rienk de Vries | Albeda | 26 | Ina Reumer | Regio College |
| 3 | Annemarie Arnaud de Calavon | Alfa College | 27 | Maarten Veldhuis | Rijn IJssel |
| 4 | Peter Mulder | AOC Terra / Og Noord | 28 | Henk Links | ROC A12 |
| 5 | Fung Yee Poon | Aventus | 29 | Joep Lemmens | ROC Arcus College |
| 6 | Martijn van Hoorn | Citaverde College | 30 | Gerrit Haakma | ROC Friese Poort |
| 7 | Floor de Ruiter | Da Vinci College | 31 | André Ridder | ROC Horizon College |
| 8 | Rene Dol | Deltion College | 32 | John Dijkman | ROC Kop van Noord Holland |
| 9 | Bert Baské | Drenthe College | 33 | Nico Hermans | ROC Leeuwenborgh |
| 10 | Harm Visser | Friesland College | 34 | René van der Mark | ROC Midden Nederland |
| 11 | Freek Beumer | Gilde Opleidingen | 35 | Sylvia Liem | ROC Mondriaan |
| 12 | Claartje Uitterhoeve | Graafschap College | 36 | Paula Cartigny | ROC Nijmegen |
| 13 | Henk Burg | Helicon Opleidingen | 37 | Gydo van Dorland | ROC MBO Rijnland |
| 14 | Willem Flink | Hoornbeek College | 38 | Stefan Geutjes | ROC Rivor |
| 15 | Jan de Hooge | Hout en Meubileringscollege  Amsterdam / Rotterdam | 39 | Theo Kuilboer | ROC Top |
| 16 | Frits Zadelhoff | Koning Willem 1 College | 40 | Co Klerkx | ROC van Amsterdam |
| 17 | Bert Lammers | Landstede | 41 | Nico Boom | Scalda |
| 18 | Rene Bosman | Lentiz Onderwijsgroep | 42 | Peter Verhoeven | Scholengemeenschap De Rooi Pannen |
| 19 | Marjolein Rombouts | MBO Utrecht | 43 | Erwin Huggers | Sint Lucas |
| 20 | Rob van Velzen | Mediacollege Amsterdam | 44 | Esther ter Avest | Soma College |
| 21 | Jelle van Bachem | Nimeto Utrecht | 45 | Frank Verkammen | Summa College |
| 22 | Linn Zuidema | Noorderpoort | 46 | Bertha Lenstra | SVO |
| 23 | Janine Kloosterman | Nordwin College | 47 | Wim Arendse | Zadkine |
| 24 | Rob Smit | Nova College |  |  |  |

**Sommige rechten voorbehouden**

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden de auteur(s), redacteur(s) en uitgever van Kennisnet geen aansprakelijkheid voor eventuele fouten of onvolkomenheden.

**Creative commons**

[](http://www.google.nl/url?sa=i&source=images&cd=&cad=rja&uact=8&ved=0CAgQjRw&url=http://creativecommons.org/about/downloads&ei=ViUYVb6yHcbWPPKhgMAM&psig=AFQjCNFD0SQUbum02GpIZCKN9_e8blqrwQ&ust=1427732182559562)Naamsvermelding 3.0 Nederland

(CC BY 3.0)

**De gebruiker mag:**

* Het werk kopiëren, verspreiden en doorgeven
* Remixen – afgeleide werken maken

**Onder de volgende voorwaarde:**

* Naamsvermelding – De gebruiker dient bij het werk de naam van Kennisnet te vermelden (maar niet zodanig dat de indruk gewekt wordt dat zij daarmee instemt met uw werk of uw gebruik van het werk).

Inhoudsopgave

[Verantwoording 2](#_Toc501637461)

[1. Conclusies IBP benchmark 2017 4](#_Toc501637462)

[1.1 Terugblik 4](#_Toc501637463)

[1.2 Representativiteit 5](#_Toc501637464)

[1.3 Benchmark ibp 2017 en algemene bevindingen ibp in het mbo 5](#_Toc501637465)

[1.4 Gedetailleerde bevindingen informatiebeveiliging 7](#_Toc501637467)

[1.5 Benchmark privacy 10](#_Toc501637469)

[1.6 Aanbevelingen (in versie 1.0 worden deze aanbevelingen concreet uitgewerkt) 11](#_Toc501637470)

[2. Resultaten ibp benchmark 12](#_Toc501637471)

[2.1 Toelichting op de tabellen 12](#_Toc501637472)

[2.2 Wat gaat goed en wat gaat minder goed? 14](#_Toc501637473)

[2.3 Beleid en organisatie 15](#_Toc501637474)

[2.4 Personeel, studenten en gasten 16](#_Toc501637475)

[2.5 Ruimtes en apparatuur 17](#_Toc501637476)

[2.6 Continuïteit 18](#_Toc501637477)

[2.7 Vertrouwelijkheid en integriteit 19](#_Toc501637478)

[2.8 Controle en Logging 20](#_Toc501637479)

[3. Benchmark compliance kader privacy 20](#_Toc501637480)

[Bijlage 1: Framework informatiebeveiliging en privacy in het mbo 22](#_Toc501637481)

# Conclusies IBP benchmark 2017

## Terugblik

Medio 2014 is de Taskforce Informatiebeveiliging en privacy van start gegaan met een duidelijke opdracht die verwoord is in het Verantwoordingsdocument[[1]](#footnote-2). 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. We willen nu graag voor het derde 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.

## Representativiteit

Aan de eerste IBP benchmark (2015) hebben 19 mbo instellingen deelgenomen. Bij de tweede benchmark (2016) waren dat al 30 mbo instellingen deelgenomen. En dit jaar hebben aan de derde benchmark (2017) 47 van de 61 mbo instellingen deelgenomen, dat is 77%.

## Benchmark ibp 2017 en algemene bevindingen ibp in het mbo

De benchmark is uitgevoerd op basis van het vastgestelde toetsingskader ibp. 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. Alle maatregelen uit het toetsingskader zijn in een zestal clusters verdeeld om het geheel overzichtelijk te maken. Cluster 1 gaat vooral over beleidsmaatregelen, cluster 2 over personeel (bewustwording), cluster drie over ruimten en apparatuur (veel ICT gerelateerde zaken), cluster 4 betreft vooral de continuïteit van de bedrijfsvoering (vooral ten aanzien van de ICT infrastructuur), cluster 5 gaat over toegang (vertrouwelijkheid) en integriteit van de data en tot slot cluster 6 dat gaat over controle en monitoring. Naast deze cluster is dit jaar voor de tweede keer ook een check uitgevoerd op een pluscluster, een extra cluster 7, dat geheel gaat over de benodigde privacy maatregelen.

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

|  |  |  |  |
| --- | --- | --- | --- |
|  | **2015** | **2016** | **2017** |
| **Cluster 1: Beleid en organisatie** | 1,7 | 1,8 | **2,0** |
| **Cluster 2: Personeel, studenten en gasten** | 1,7 | 1,7 | **1,9** |
| **Cluster 3: Ruimtes en apparatuur** | 2,1 | 2,2 | **2,3** |
| **Cluster 4: Continuïteit** | 2,0 | 2,1 | **2,3** |
| **Cluster 5: Vertrouwelijkheid en integriteit** | 2,0 | 2,0 | **2,2** |
| **Cluster 6: Controle en Logging** | 1,6 | 1,6 | **1,8** |
| **Totaal score Informatiebeveiliging in de mbo sector** | **1,9** | **1,9** | **2,1** |
|  |  |  |  |
| **Totaal score Privacy in de mbo sector** | **-** | **1,5** | **1,9** |

Bron: Benchmark ibp in het mbo 2017, Kennisnet en saMBO-ICT (december 2017)

Ook is er gekeken naar de ontwikkelingen in relatie tot de instellingen die al drie keer, twee keer of dit jaar juist voor de eerste keer hebben meegedaan. In kolom 2, 3 en 4 staan de resultaten van de resultaten van de mbo instellingen die 3 maal hebben deelgenomen, in kolom 4 en 5 de mbo instellingen die 2 maal hebben deelgenomen. In de laatste kolom de mbo instellingen die voor de eerste maal hebben deelgenomen.

Zoals verwacht zijn de nieuwe instellingen nog iets lager in de scores dan de instellingen die al langer ibp op de agenda hebben staan.

# 

# 

Als mbo sector hebben wij ons een gemiddelde score van 2 tot doel gesteld. Deze doelstelling is gehaald.

De “technische” clusters (ruimten en apparatuur, continuïteit, vertrouwelijkheid en integriteit) scoren een ruime 2. Dat mocht ook verwacht worden gezien het feit dat de instellingen in het mbo de technische zaken wel op orde hebben. Waar het vaak nog aan ontbreekt is de documentatie hiervan maar de maatregelen zijn over het algemeen wel getroffen. Dat is een pluspunt in de benchmark. Wel is het cluster “Controle en logging” onder de maat. Dit heeft ook de afgelopen periode niet de prioriteit gehad, daar moet in de komende jaren in het kader van ‘in control zijn’ en ook op het gebied van incident management nog veel aan gebeuren.

Zorgelijk blijft dat de nieuwkomers op het cluster “Beleid en organisatie” slechts 1,8 scoren. Met andere woorden het beleid is nog niet op orde. Dit geldt ook voor scholing en awareness van medewerkers, studenten en gasten. Alleen de mbo instellingen die voor de derde maal meedoen scoren hier een 2,1.

De privacy score (1,9) is teleurstellend. Wel hebben verschillende mbo instellingen aangegeven dat de komende maanden hard gewerkt wordt om op 25 mei 2018 te voldoen aan de Europese ‘Algemene Verordening Gegevensbescherming (AVG)’.

## Gedetailleerde bevindingen informatiebeveiliging



Momenteel zijn er in Nederland 61 mbo instellingen. In de wetenschap dat AOC Oost en Groene Welle gaan fuseren zullen er op korte termijn 60 instellingen over blijven.

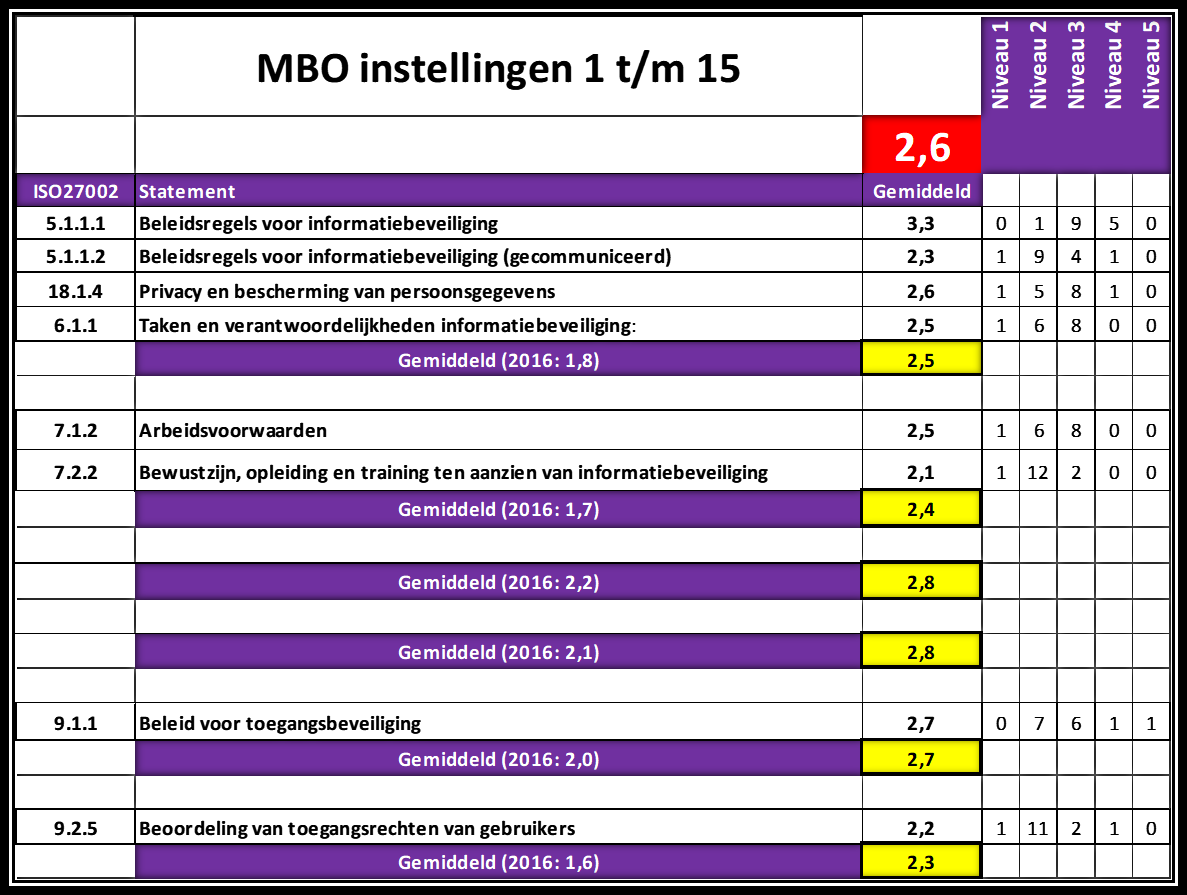
Om inzicht te krijgen in de stand van zaken op het gebied van informatiebeveiliging binnen de mbo sector zijn deze 60 instellingen verdeeld in 4 kwartielen van ieder 15 instellingen.

Om de cijfers betrouwbaar te maken is voor de volgende aanpak gekozen.

* De cijfers van de 47 deelnemende instellingen zijn uiteraard meegenomen.
* 4 mbo instellingen hebben in het verleden deelgenomen maar nu niet. De cijfers uit het verleden zijn meegenomen.
* Van 51 instellingen zijn dus cijfers beschikbaar. 9 instellingen hebben nooit deelgenomen aan de benchmark en zijn dan ook gewaardeerd op 1.

Opbouw:

* Het eerste kwartiel bevat de resultaten van de 15 mbo instellingen met de gemiddeld hoogste score van de 51 beschikbare mbo scores.
* Het tweede en derde kwartiel zijn een weergave van de scores 16 t/m 30 en 31 t/m 45.
* Het vierde kwartiel bevat de scores van de 6 laagste deelnemende mbo instellingen en de 9 niet deelnemers (met de fictieve score 1). Dit vierde kwartiel is niet opgenomen in het overzicht vanwege de onbetrouwbare score van niet deelnemende mbo instellingen.



## 

## Benchmark privacy

Dit jaar is er naast informatiebeveiliging, voor de tweede keer getoetst op privacy. De benchmark is uitgevoerd op basis van het vastgestelde toetsingskader privacy[[2]](#footnote-3).

De gemiddelde score van de benchmark privacy bedraagt 1,9. 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. Toch zijn er een tweetal pluspunten te benoemen:

* Vorig jaar scoorde de mbo sector 1,5, met andere woorden een verbetering van 0,4.
* Veel mbo instellingen hebben aangegeven dat hun score, medio 2018, fors zal verbeteren. Tijdens de netwerkbijeenkomst in december 2017, gaven de daar aanwezige mbo instellingen aan dat ze per

25-5-2018 over een FG’er beschikken, terwijl in de benchmark dat slechts de helft is.



## Samenvatting benchmark in de afgelopen jaren

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Cluster nummer** | **Cluster titel** | **HO**  **2011** | **HO**  **2013** | **HO**  **2015** | **HO**  **2017** | **MBO**  **2015** | **MBO**  **2016** | **MBO**  **2017** |
| **1 t/m 6** | **Totaal informatiebeveiliging** | **2.0** | **2.2** | **2.4** | **2,4** | **1.9** | **1,9** | **2,1** |
| 1 | Beleid en organisatie | 2.0 | 2.2 | 2.4 | 2,4 | 1.7 | 1,8 | 2,0 |
| 2 | Personeel, gasten, studenten | 2.1 | 2.2 | 2.1 | 2,2 | 1.7 | 1,7 | 1,9 |
| 3 | Ruimtes en apparatuur | 2.0 | 2.4 | 2.7 | 2,5 | 2.1 | 2,2 | 2,3 |
| 4 | Continuïteit | 2.3 | 2.4 | 2.6 | 2,6 | 2.0 | 2,1 | 2,3 |
| 5 | Toegangsbeveiliging en integriteit | 2.1 | 2.2 | 2.4 | 2,6 | 2.0 | 2,0 | 2,2 |
| 6 | Controle en logging | 1.5 | 2.0 | 2.2 | 2,1 | 1.6 | 1,6 | 1,8 |
|  | | | | | | | | |
| **7** | **Privacy** |  | | | | | **1,5** | **1,9** |

## Aanbevelingen

Op basis van de benchmark komen de 47 deelnemende mbo instellingen tot de volgende aanbevelingen:

* Training voor proceseigenaren organiseren
* Wat doe je bij incidenten? Incidenten delen en wat heb je dan gedaan?
* Opleveren (model) verwerkersovereenkomsten voor de 10 meest gebruikte applicaties in de mbo sector. Aangezien veel mbo-instellingen van de zelfde partijen gebruik maken, heeft het bundelen van expertise om gezamenlijk de bewerkersovereenkomst te toetsen cq. af te stemmen de voorkeur. Er is reeds een initiatief hiertoe gestart.
* Aanpassen toetsingskaders aan nieuwe ontwikkelingen
* Opzetten Masterclass Privacy vanuit de praktijk
* Het classificeren en labelen van gegevens verdient extra aandacht. In de onderwijspraktijk blijkt dit voor meerdere organisaties lastig om praktisch in te vullen. In samenhang met het voorgaande punt wordt dit uitgewerkt en toegelicht in de voornoemde handleiding
* MBO-instellingen hebben het afgelopen jaar vragen gesteld over het delen van leerling gegevens met externe partijen. Voorbeelden zijn de JOB Monitor, Cultureel Jongeren Pas, MBO Studentenpas, gegevens naar VO scholen t.b.v. warme overdracht, etc… Er zal onderzocht worden of in alle gevallen toestemming nodig is van leerling/ouder om deze gegevens te mogen versturen. Er wordt onderzocht hoe deze de toestemming op een makkelijke, maar legitieme manier kan worden geregeld (aanhakend bij lopende initiatieven zoals het digitaal aanmeld formulier).
* Ontwikkelen van een beleidsdocument Controle en Logging..
* Het is wenselijk dat in 2018 alle mbo instellingen deelnemen aan de benchmark. Op verzoek van de Stuurgroep is de lijst toegevoegd van de mbo instellingen die niet hebben deelgenomen:

|  |  |  |
| --- | --- | --- |
| AOC de Groene Welle \* | Grafisch Lyceum Utrecht \* | ROC van Twente |
| AOC Oost \* | Leidse Instrumentmakersschool \* | ROC West Brabant |
| CIBAP vakschool voor verbeelding \* | MBO Amersfoort \* | STC-Group \* |
| Clusius College | ROC De Leijgraaf \* | Wellantcollege \* |
| Grafisch Lyceum Rotterdam | ROC Ter AA \* |  |

\* 10 (van de 61) mbo instellingen hebben nog nooit deelgenomen aan de benchmark ibp.

# Resultaten ibp benchmark

## Toelichting op de tabellen

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

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | **Niveau 1** | **Niveau 2** | **Niveau 3** | **Niveau 4** | **Niveau 5** |  |
| **Nr.** | **ISO27002** | **Statement** | **2017** |  |  |  |  |  | **2016** |
| **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.



|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | **Niveau 1** | **Niveau 2** | **Niveau 3** | **Niveau 4** | **Niveau 5** |  |
| **Nr.** | **ISO27002** | **Statement** | **2017** |  |  |  |  |  | **2016** |
| **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.

Het gemiddelde cijfer (2017 en 2016) is het rekenkundige gemiddelde van de individuele waarnemingen.

## Wat gaat goed en wat gaat minder goed?

**Best scorende statements uit alle clusters.**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | **Niveau 1** | **Niveau 2** | **Niveau 3** | **Niveau 4** | **Niveau 5** |
| **Nr.** | **ISO27002** | **Statement** | **2017** |  |  |  |  |  |
| **4.5** | **12.3.1.1** | **Back-up van informatie** | **2,9** | **1** | **10** | **27** | **9** | **0** |
| **5.3** | **9.2.1** | **Registratie en afmelden van gebruikers** | **2,7** | **3** | **18** | **19** | **4** | **3** |
| **3.15** | **12.4.4** | **Kloksynchronisatie** | **2,7** | **3** | **16** | **22** | **5** | **1** |
| **4.3** | **12.2.1.1** | **Beheersmaatregelen tegen malware** | **2,7** | **0** | **22** | **19** | **6** | **0** |
| **3.10** | **11.2.2** | **Nutsvoorzieningen** | **2,7** | **4** | **13** | **24** | **5** | **0** |
| **5.13** | **13.1.1** | **Beheersmaatregelen voor netwerken** | **2,6** | **3** | **18** | **22** | **2** | **2** |
| **5.15** | **13.1.3** | **Scheiding in netwerken** | **2,5** | **5** | **16** | **23** | **2** | **1** |
| **3.12** | **11.2.4** | **Onderhoud van apparatuur** | **2,5** | **2** | **24** | **17** | **3** | **1** |

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.**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | **Niveau 1** | **Niveau 2** | **Niveau 3** | **Niveau 4** | **Niveau 5** |
| **Nr.** | **ISO27002** | **Statement** | **2017** |  |  |  |  |  |
| **1.8** | **8.2.2** | **Informatie labelen** | **1,4** | **27** | **19** | **1** | **0** | **0** |
| **1.7** | **8.2.1** | **Classificatie van informatie** | **1,5** | **27** | **18** | **2** | **0** | **0** |
| **6.3** | **12.4.3** | **Logbestanden van beheerders en operators** | **1,6** | **23** | **21** | **3** | **0** | **0** |
| **1.5** | **6.1.5** | **Informatiebeveiliging in projectbeheer** | **1,6** | **22** | **21** | **4** | **0** | **0** |
| **1.10** | **10.1.1.2** | **Beleid inzake het gebruik van cryptografische beheersmaatregelen** | **1,6** | **25** | **16** | **5** | **1** | **0** |
| **4.14** | **17.1.2** | **Informatiebeveiligingscontinuïteit implementeren** | **1,6** | **23** | **19** | **5** | **0** | **0** |
| **5.11** | **10.1.2.2** | **Sleutelbeheer** | **1,6** | **24** | **18** | **4** | **1** | **0** |
| **1.9** | **10.1.1.1** | **Beleid inzake het gebruik van cryptografische beheersmaatregelen** | **1,6** | **25** | **15** | **6** | **1** | **0** |
| **2.2** | **7.2.2** | **Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging** | **1,6** | **22** | **20** | **5** | **0** | **0** |

Cluster 3 kent geen statement dat zeer slecht scoort. Cluster 1, beleid, komt viermaal voor. **2.2 scoort te slecht**.

## Beleid en organisatie

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | **Niveau 1** | **Niveau 2** | **Niveau 3** | **Niveau 4** | **Niveau 5** |  |
| **Nr.** | **ISO27002** | **Statement** | **2017** |  |  |  |  |  | **2016** |
| **1.1** | **5.1.1.1** | **Beleidsregels voor informatiebeveiliging** | **2,4** | **9** | **14** | **19** | **5** | **0** | **2,2** |
| **1.2** | **5.1.1.2** | **Beleidsregels voor informatiebeveiliging (gecommuniceerd)** | **1,7** | **20** | **20** | **6** | **1** | **0** | **1,6** |
| **1.3** | **5.1.2** | **Beoordeling van het Informatiebeveiligingsbeleid** | **1,9** | **20** | **16** | **5** | **6** | **0** | **1,7** |
| **1.4** | **6.1.1** | **Taken en verantwoordelijkheden informatiebeveiliging**: | **2,0** | **11** | **24** | **11** | **1** | **0** | **2,2** |
| **1.5** | **6.1.5** | **Informatiebeveiliging in projectbeheer** | **1,6** | **22** | **21** | **4** | **0** | **0** | **1,6** |
| **1.6** | **6.2.1.1** | **Beleid voor mobiele apparatuur:** | **2,0** | **12** | **24** | **10** | **1** | **0** | **1,9** |
| **1.7** | **8.2.1** | **Classificatie van informatie** | **1,5** | **27** | **18** | **2** | **0** | **0** | **1,4** |
| **1.8** | **8.2.2** | **Informatie labelen** | **1,4** | **27** | **19** | **1** | **0** | **0** | **1,5** |
| **1.9** | **10.1.1.1** | **Beleid inzake het gebruik van cryptografische beheersmaatregelen** | **1,6** | **25** | **15** | **6** | **1** | **0** | **1,5** |
| **1.10** | **10.1.1.2** | **Beleid inzake het gebruik van cryptografische beheersmaatregelen** | **1,6** | **25** | **16** | **5** | **1** | **0** | **1,4** |
| **1.11** | **11.2.5** | **Verwijdering van bedrijfsmiddelen** | **2,1** | **12** | **21** | **11** | **2** | **1** | **1,8** |
| **1.12** | **13.2.1** | **Beleid en procedures voor informatietransport:** | **1,9** | **14** | **24** | **8** | **1** | **0** | **1,6** |
| **1.13** | **13.2.2** | **Overeenkomsten over informatietransport** | **2,3** | **7** | **21** | **17** | **2** | **0** | **1,8** |
| **1.14** | **14.1.1** | **Analyse en specificatie van informatiebeveiligingseisen** | **2,0** | **10** | **25** | **12** | **0** | **0** | **1,9** |
| **1.15** | **15.1.2** | **Opnemen van beveiligingsaspecten in leveranciersovereenkomsten** | **2,0** | **10** | **28** | **8** | **1** | **0** | **1,8** |
| **1.16** | **15.1.3** | **Toeleveringsketen van informatie- en communicatietechnologie** | **2,0** | **11** | **26** | **10** | **0** | **0** | **1,9** |
| **1.17** | **16.1.1** | **Verantwoordelijkheden en procedures**. | **2,3** | **7** | **21** | **17** | **2** | **0** | **2,0** |
| **1.18** | **16.1.2** | **Rapportage van informatiebeveiligingsgebeurtenissen** | **2,3** | **12** | **13** | **19** | **3** | **0** | **2,1** |
| **1.19** | **18.1.3** | **Beschermen van registraties** | **1,8** | **16** | **24** | **7** | **0** | **0** | **1,7** |
| **1.20** | **18.1.4** | **Privacy en bescherming van persoonsgegevens** | **2,1** | **7** | **28** | **11** | **1** | **0** | **2,0** |
| **1.21** | **6.1.2** | **Scheiding van taken** | **2,1** | **8** | **28** | **11** | **0** | **0** | **2,0** |
|  |  | **Gemiddeld (2016: 1,8)** | **1,9** |  |  |  |  |  |  |

## Personeel, studenten en gasten

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | **Niveau 1** | **Niveau 2** | **Niveau 3** | **Niveau 4** | **Niveau 5** |  |
| **Nr.** | **ISO27002** | **Statement** | **2017** |  |  |  |  |  | **2016** |
| **2.1** | **7.1.2** | **Arbeidsvoorwaarden** | **1,9** | **15** | **22** | **10** | **0** | **0** | **2,0** |
| **2.2** | **7.2.2** | **Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging** | **1,6** | **22** | **20** | **5** | **0** | **0** | **1,4** |
| **2.3** | **9.2.6** | **Toegangsrechten intrekken of aanpassen** | **2,2** | **8** | **22** | **16** | **1** | **0** | **2,3** |
| **2.4** | **11.2.9** | **‘Clear desk’- en ‘clear screen’-beleid** | **1,7** | **20** | **21** | **5** | **1** | **0** | **1,6** |
| **2.5** | **13.2.4** | **Vertrouwelijkheids- of geheimhoudingsovereenkomst** | **1,8** | **14** | **28** | **4** | **1** | **0** | **1,6** |
| **2.6** | **16.1.3** | **Rapportage van zwakke plekken in de informatiebeveiliging** | **1,7** | **21** | **21** | **4** | **1** | **0** | **1,5** |
| **2.7** | **7.1.1** | **Screening** | **2,3** | **5** | **28** | **11** | **2** | **1** | **1,8** |
|  |  | **Gemiddeld (2016: 1,7)** | **1,9** |  |  |  |  |  |  |

## Ruimtes en apparatuur

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | **Niveau 1** | **Niveau 2** | **Niveau 3** | **Niveau 4** | **Niveau 5** |  |
| **Nr.** | **ISO27002** | **Statement** | **2017** |  |  |  |  |  | **2016** |
| **3.1** | **6.1.2.1** | **Beleid voor mobiele apparatuur** | **2,1** | **10** | **26** | **8** | **3** | **0** | **2,1** |
| **3.2** | **8.3.2** | **Verwijderen van media** | **2,1** | **8** | **28** | **9** | **2** | **0** | **2,0** |
| **3.3** | **11.1.1** | **Fysieke beveiligingszone** | **2,4** | **3** | **23** | **20** | **1** | **0** | **2,2** |
| **3.4** | **11.1.2** | **Fysieke toegangsbeveiliging** | **2,3** | **4** | **29** | **12** | **2** | **0** | **2,0** |
| **3.5** | **11.1.3** | **Kantoren, ruimten en faciliteiten beveiligen** | **2,2** | **3** | **33** | **9** | **2** | **0** | **2,0** |
| **3.6** | **11.1.4** | **Beschermen tegen bedreigingen van buitenaf** | **2,4** | **3** | **27** | **13** | **4** | **0** | **2,3** |
| **3.7** | **11.1.5** | **Werken in beveiligde gebieden** | **2,1** | **7** | **31** | **6** | **3** | **0** | **2,0** |
| **3.8** | **11.1.6** | **Laad- en loslocatie** | **2,0** | **10** | **27** | **8** | **2** | **0** | **1,9** |
| **3.9** | **11.2.1** | **Plaatsing en bescherming van apparatuur** | **2,3** | **0** | **34** | **10** | **3** | **0** | **2,3** |
| **3.10** | **11.2.2** | **Nutsvoorzieningen** | **2,7** | **4** | **13** | **24** | **5** | **0** | **2,5** |
| **3.11** | **11.2.3** | **Beveiliging van bekabeling** | **2,4** | **2** | **25** | **17** | **3** | **0** | **2,3** |
| **3.12** | **11.2.4** | **Onderhoud van apparatuur** | **2,5** | **2** | **24** | **17** | **3** | **1** | **2,4** |
| **3.13** | **11.2.6** | **Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein** | **2,1** | **7** | **26** | **14** | **0** | **0** | **1,9** |
| **3.14** | **11.2.7** | **Veilig verwijderen of hergebruiken van apparatuur** | **2,3** | **3** | **29** | **13** | **2** | **0** | **1,9** |
| **3.15** | **12.4.4** | **Kloksynchronisatie** | **2,7** | **3** | **16** | **22** | **5** | **1** | **2,4** |
|  |  | **Gemiddeld (2016: 2,2)** | **2,3** |  |  |  |  |  |  |

## Continuïteit

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | **Niveau 1** | **Niveau 2** | **Niveau 3** | **Niveau 4** | **Niveau 5** |  |
| **Nr.** | **ISO27002** | **Statement** | **2017** |  |  |  |  |  | **2016** |
| **4.1** | **12.1.2** | **Wijzigingsbeheer** | **2,4** | **4** | **24** | **14** | **5** | **0** | **2,3** |
| **4.2** | **12.1.4** | **Scheiding van ontwikkel-, test- en productieomgevingen** | **2,2** | **5** | **30** | **9** | **3** | **0** | **2,2** |
| **4.3** | **12.2.1.1** | **Beheersmaatregelen tegen malware** | **2,7** | **0** | **22** | **19** | **6** | **0** | **2,6** |
| **4.4** | **12.2.1.2** | **Beheersmaatregelen tegen malware** | **2,2** | **8** | **20** | **19** | **0** | **0** | **1,8** |
| **4.5** | **12.3.1.1** | **Back-up van informatie** | **2,9** | **1** | **10** | **27** | **9** | **0** | **2,9** |
| **4.6** | **12.3.1.2** | **Back-up van informatie** | **2,2** | **8** | **22** | **16** | **1** | **0** | **2,2** |
| **4.7** | **12.5.1** | **Software installeren op operationele systemen** | **2,3** | **3** | **29** | **11** | **4** | **0** | **2,5** |
| **4.8** | **12.6.1** | **Beheer van technische kwetsbaarheden** | **2,1** | **10** | **23** | **14** | **0** | **0** | **1,7** |
| **4.9** | **12.6.2** | **Beperkingen voor het installeren van software** | **2,4** | **9** | **14** | **22** | **1** | **1** | **2,5** |
| **4.10** | **14.2.6** | **Beveiligde ontwikkelomgeving** | **2,2** | **8** | **24** | **12** | **3** | **0** | **1,9** |
| **4.11** | **15.2.2** | **Beheer van veranderingen in dienstverlening van leveranciers** | **2,1** | **6** | **30** | **10** | **1** | **0** | **1,8** |
| **4.12** | **16.1.4** | **Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen** | **2,1** | **9** | **26** | **10** | **2** | **0** | **1,8** |
| **4.13** | **16.1.5** | **Respons op informatiebeveiligingsincidenten** | **2,3** | **9** | **22** | **11** | **5** | **0** | **2,0** |
| **4.14** | **17.1.2** | **Informatiebeveiligingscontinuïteit implementeren** | **1,6** | **23** | **19** | **5** | **0** | **0** | **1,4** |
| **4.15** | **17.2.1** | **Beschikbaarheid van informatie verwerkende faciliteiten** | **2,2** | **7** | **25** | **12** | **3** | **0** | **1,8** |
|  |  | **Gemiddeld (2016: 2,1)** | **2,3** |  |  |  |  |  |  |

## Vertrouwelijkheid en integriteit

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | **Niveau 1** | **Niveau 2** | **Niveau 3** | **Niveau 4** | **Niveau 5** |  |
| **Nr.** | **ISO27002** | **Statement** | **2017** |  |  |  |  |  | **2016** |
| **5.1** | **9.1.1** | **Beleid voor toegangsbeveiliging** | **2,2** | **5** | **29** | **11** | **1** | **1** | **2,2** |
| **5.2** | **9.1.2** | **Toegang tot netwerken en netwerkdiensten** | **2,4** | **4** | **23** | **18** | **2** | **0** | **2,3** |
| **5.3** | **9.2.1** | **Registratie en afmelden van gebruikers** | **2,7** | **3** | **18** | **19** | **4** | **3** | **2,3** |
| **5.4** | **9.2.2** | **Gebruikers toegang verlenen** | **2,3** | **3** | **30** | **12** | **1** | **1** | **2,0** |
| **5.5** | **9.2.3** | **Beheren van speciale toegangsrechten** | **2,1** | **4** | **36** | **6** | **1** | **0** | **2,1** |
| **5.6** | **9.2.4** | **Beheer van geheime authenticatie-informatie van gebruikers** | **2,2** | **8** | **20** | **19** | **0** | **0** | **2,1** |
| **5.7** | **9.3.1** | **Geheime authenticatie-informatie gebruiken** | **2,4** | **7** | **20** | **14** | **6** | **0** | **1,9** |
| **5.8** | **9.4.1** | **Beperking toegang tot informatie** | **2,1** | **5** | **33** | **9** | **0** | **0** | **2,2** |
| **5.9** | **9.4.2** | **Beveiligde inlogprocedures** | **2,3** | **4** | **27** | **15** | **1** | **0** | **2,4** |
| **5.10** | **10.1.2.1** | **Sleutelbeheer** | **1,7** | **20** | **24** | **2** | **1** | **0** | **1,4** |
| **5.11** | **10.1.2.2** | **Sleutelbeheer** | **1,6** | **24** | **18** | **4** | **1** | **0** | **1,5** |
| **5.12** | **12.4.2** | **Beschermen van informatie in logbestanden** | **1,7** | **21** | **22** | **3** | **1** | **0** | **1,6** |
| **5.13** | **13.1.1** | **Beheersmaatregelen voor netwerken** | **2,6** | **3** | **18** | **22** | **2** | **2** | **2,5** |
| **5.14** | **13.1.2** | **Beveiliging van netwerkdiensten** | **2,3** | **7** | **22** | **16** | **2** | **0** | **2,0** |
| **5.15** | **13.1.3** | **Scheiding in netwerken** | **2,5** | **5** | **16** | **23** | **2** | **1** | **2,3** |
| **5.16** | **13.2.3** | **Elektronische berichten** | **2,1** | **7** | **27** | **12** | **1** | **0** | **1,9** |
| **5.17** | **14.1.3** | **Transacties van toepassingen beschermen** | **2,0** | **11** | **27** | **7** | **2** | **0** | **1,6** |
|  |  | **Gemiddeld (2015: 2,0)** | **2,2** |  |  |  |  |  |  |

## Controle en Logging

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | **Niveau 1** | **Niveau 2** | **Niveau 3** | **Niveau 4** | **Niveau 5** |  |
| **Nr.** | **ISO27002** | **Statement** | **2017** |  |  |  |  |  | **2016** |
| **6.1** | **9.2.5** | **Beoordeling van toegangsrechten van gebruikers** | **1,8** | **12** | **32** | **2** | **1** | **0** | **1,8** |
| **6.2** | **12.4.1** | **Gebeurtenissen registreren** | **1,8** | **14** | **30** | **3** | **0** | **0** | **1,7** |
| **6.3** | **12.4.3** | **Logbestanden van beheerders en operators** | **1,6** | **23** | **21** | **3** | **0** | **0** | **1,6** |
| **6.4** | **14.2.7** | **Uitbestede softwareontwikkeling** | **2,1** | **15** | **19** | **7** | **6** | **0** | **1,6** |
| **6.5** | **14.2.8** | **Testen van systeembeveiliging** | **1,8** | **23** | **14** | **8** | **2** | **0** | **1,4** |
| **6.6** | **14.2.9** | **Systeemacceptatietests** | **2,2** | **7** | **25** | **13** | **2** | **0** | **2,0** |
| **6.7** | **15.2.1** | **Monitoring en beoordeling van dienstverlening van leveranciers** | **1,8** | **18** | **20** | **9** | **0** | **0** | **1,6** |
| **6.8** | **16.1.7** | **Verzamelen van bewijsmateriaal** | **1,7** | **20** | **21** | **6** | **0** | **0** | **1,5** |
| **6.9** | **18.2.2** | **Naleving van beveiligingsbeleid en –normen** | **1,7** | **17** | **29** | **1** | **0** | **0** | **1,5** |
| **6.10** | **18.2.3** | **Beoordeling van technische naleving** | **1,8** | **17** | **25** | **4** | **1** | **0** | **1,5** |
|  |  | **Gemiddeld (2015: 1,6)** | **1,8** |  |  |  |  |  |  |

# Benchmark compliance kader privacy

De uitkomst van de privacy benchmark is teleurstellend. Alleen datalekken scoort (althans de mediaan) op volwassenheidsniveau 3.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Statements compliance-kader privacy** | |  |  | **Niveau 1** | **Niveau 2** | **Niveau 3** | **Niveau 4** | **Niveau 5** |
| **1     Beleid en organisatie** | | **1,9** |  |  |  |  |  |  |
| **Nr.** | **Statement** |  |  |  |  |  |  |  |
| **P.1** | **Privacy-beleid**: | **2,2** |  | **5** | **15** | **10** | **1** | **0** |
| **P.2** | **Functionaris gegevensbescherming:** | **2,0** |  | **15** | **6** | **6** | **4** | **0** |
| **P.3** | **Doelbepaling, doelbinding, grondslag, grond bij minderjarigen en dataminimalisatie.** | **1,7** |  | **15** | **11** | **2** | **2** | **0** |
| **P.4** | **Registratieplicht:** | **1,5** |  | **22** | **5** | **3** | **1** | **0** |
| **P.5** | **Bewaartermijnen:** | **1,5** |  | **18** | **11** | **1** | **1** | **0** |
| **P.6** | **Verwerking t.b.v. onderzoek:** | **1,5** |  | **21** | **5** | **4** | **1** | **0** |
| **P.7** | **Verwerking van bijzondere persoonsgegevens:** | **1,8** |  | **15** | **10** | **3** | **3** | **0** |
| **P.8** | **Geautomatiseerde besluitvorming:** | **1,7** |  | **20** | **4** | **4** | **2** | **1** |
| **P.9** | **Informatiebeveiliging**: | **2,1** |  | **7** | **15** | **8** | **1** | **0** |
| **P.10** | **Bewerkersovereenkomsten**: | **2,0** |  | **8** | **17** | **5** | **1** | **0** |
| **2     Personeel, studenten en gasten** | |  |  |  |  |  |  |  |
| **Nr.** | **Statement** |  |  |  |  |  |  |  |
| **P.11** | **Transparantie privacy beleid:** | **2,0** |  | **11** | **11** | **8** | **1** | **0** |
| **P.12** | **Informatieplicht verwerkingen:** | **1,6** |  | **14** | **14** | **2** | **0** | **0** |
| **P.13** | **Rechten van betrokkene:** | **1,8** |  | **12** | **12** | **5** | **1** | **0** |
| **P.14** | **Arbeidsvoorwaarden**: | **2,3** |  | **5** | **16** | **5** | **3** | **1** |
| **P.15** | **Bewustzijn, opleiding en training ten aanzien van privacy:** | **1,5** |  | **18** | **12** | **1** | **0** | **0** |
| **3     Ruimtes en apparatuur** | |  |  |  |  |  |  |  |
| **Nr.** | **Statement** |  |  |  |  |  |  |  |
| **P.16** | **Verwijderen van persoonsgegevens:** | **2,4** |  | **3** | **17** | **7** | **4** | **0** |
| **4     Vertrouwelijkheid en integriteit** | |  |  |  |  |  |  |  |
| **Nr.** | **Statement** |  |  |  |  |  |  |  |
| **P.17** | **Datakwaliteit (data-integriteit):** | **2,2** |  | **4** | **19** | **7** | **1** | **0** |
| **P.18** | **Datalek:** | **2,5** |  | **5** | **10** | **12** | **3** | **1** |
| **P.19** | **Bijzondere persoonsgegevens:** | **2,1** |  | **5** | **19** | **6** | **1** | **0** |
| **5     Controle en logging** | |  |  |  |  |  |  |  |
| **Nr.** | **Statement** |  |  |  |  |  |  |  |
| **P.20** | **Privacy in informatiesystemen**: | **1,7** |  | **12** | **15** | **4** | **0** | **0** |
| **P.21** | **Gegevensbeschermingseffectbeoordeling (GEB, voorheen PIA):** | **1,4** |  | **22** | **6** | **3** | **0** | **0** |
| **P.22** | **Naleving van privacy beleid en –normen:** | **1,5** |  | **16** | **13** | **2** | **0** | **0** |
| **P.23** | **Rapportage van privacy-gebeurtenissen**: | **2,3** |  | **6** | **13** | **10** | **2** | **0** |
| **P.24** | **Gebeurtenissen registreren:** | **1,9** |  | **13** | **10** | **7** | **1** | **0** |

Bijlage 1: Framework informatiebeveiliging en privacy in het mbo

****

1. Zie IBPDOC1: Verantwoordingsdocument Informatiebeveiliging en privacy (ibp) in het mbo. [↑](#footnote-ref-2)
2. IBPDOC7: Toetsingskader privacy: cluster 7 [↑](#footnote-ref-3)