**Verantwoordingsdocument**

**informatiebeveiliging en privacy (ibp) in het mbo.**

****

**IBPDOC1**

**Auteurs**

Leo Bakker (Kennisnet)

Ludo Cuijpers (Leeuwenborgh Opleidingen)

Axel Eissens (Kennisnet)

Versie 2.5 augustus 2016

**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**

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

[1. Inleiding 4](#_Toc460602245)

[2. Framework informatiebeveiliging en privacy in het mbo 6](#_Toc460602246)

[2.1 Onderdelen van het framework 6](#_Toc460602247)

[2.1.1 Normenkaders…………………………………………………………………………………………………………….6](#_Toc460602248)

[2.1.2 Toetsingskaders………………………………………………………………………………………………………….7](#_Toc460602249)

[2.1.3 Handreikingen…………………………………………………………………………………………………………….8](#_Toc460602250)

[3. Beheersing, audits en benchmark 9](#_Toc460602251)

[4. Samenwerking en afstemming in het mbo 11](#_Toc460602252)

[5. De praktijk 12](#_Toc460602253)

[5.1 Interview met Ben Geerdink. 12](#_Toc460602254)

[5.2 Interview met Martien van Beekveld 13](#_Toc460602255)

[Overzicht: 14](#_Toc460602256)

# Inleiding

Het onderwerp informatiebeveiliging en privacy (ibp) is in korte tijd hoog op de agenda van het mbo gekomen. In het onderwijs worden steeds meer gegevens bijgehouden en de mbo-sector realiseert zich hoe belangrijk het is om op een goede en veilige manier met deze informatie om te gaan. Dit geldt zeker voor alle persoonsgegevens die de mbo-instelling beheert. Deelnemers en medewerkers mogen ervan uitgaan dat de instelling hun gegevens zorgvuldig behandelt en het geschonken vertrouwen niet beschaamt. Daarnaast is het van belang dat het mbo zijn primaire rol op een betrouwbare en correcte wijze uitvoert. Namelijk: goed onderwijs geven en studenten diplomeren. Diploma’s zijn maatschappelijk van grote waarde en mogen nooit ter discussie komen te staan.

Tot voor kort was de aanpak daarvoor nog heel beperkt en gebrekkig. Er waren afspraken nodig om de te nemen maatregelen te relateren aan normen en compliancekaders. Hiermee kan uiteindelijk ook worden beoordeeld in welke mate het mbo aan die normen en kaders voldoet. Het programma ibp in het mbo is gestart in september 2014 en heeft in december 2015 de eerste resultaten opgeleverd. Deze zijn in 2016 nog een keer nauwkeurig gereviseerd. Dit document geeft de verantwoording weer van dat programma en geeft kort een overzicht van de resultaten en verdere stappen om ibp in het mbo succesvol verder te implementeren. Daarnaast zijn alle relevante documenten, normen en kaders, handreikingen en informatie die voor ibp in het mbo belangrijk zijn bijeengebracht in het zogenaamde ‘framework ibp in het mbo’. De bijgaande box ‘informatiebeveiliging en privacy in het mbo’ is daar een tastbare weergave van.

Binnen het programma ibp is een aantal stakeholders benoemd. De belangrijkste zijn:

* **Mbo-instellingen**; de mbo-instellingen zijn verenigd in en vertegenwoordigd door de MBO Raad. Het is belangrijk dat de instellingen hun verantwoordelijkheid (kunnen) nemen in deze complexe materie en dat zij op maatschappelijk verantwoorde wijze met gegevens omgaan. Iedereen binnen de instellingen is daarvoor verantwoordelijk en het bewustzijn daarvan is cruciaal. De uiteindelijke verantwoordelijkheid ligt bij het College van Bestuur. Gezien de sectorale aanpak is het van belang dat ibp bestuurlijk breed wordt gedragen en dat ibp in het mbo samen met saMBO-ICT en de MBO Raad gemeenschappelijk wordt versterkt. De aanpak begint met bestuurders die zich bewust zijn van de essentie en strekking van ibp.
* **Ministerie van OCW**; vertegenwoordigers van OCW hebben in juni 2014 tijdens een bijeenkomst met het onderwijsveld zorgen geuit ten aanzien van informatiebeveiliging. Incidenten met examens, die op straat terecht kwamen, gaven daar aanleiding toe. Ook hadden ze behoefte aan meer inzicht in hoe de onderwijssector er voor staat op het gebied van informatiebeveiliging. Dat beeld ontbrak grotendeels. Het ministerie gaf aan graag te zien dat de mbo-sector dat beeld helder gaat weergeven en dat de sector maatregelen treft om de informatiebeveiliging en privacy bescherming te verbeteren en vervolgens deze te garanderen. Op grond van afspraken zou de Inspectie van het Onderwijs dan ook in staat moeten zijn om op afstand controle uit te oefenen. Het ministerie is akkoord gegaan met deze sectorale aanpak en ondersteunt initiatieven om hierbij ook significante voortgang te boeken.
* **Externe partijen, waaronder:**
	+ *ondersteunende organisaties voor de sector;* Kennisnet en SURF ondersteunen de mbo-sector vanuit een directe aansturing door een gebruikersgroep ibp in het mbo (zie ook hoofdstuk 6). Op het terrein van informatiebeveiliging en privacy worden zij aangesproken om hun expertise beschikbaar te stellen en te ondersteunen bij de realisatie van de doelstellingen in onze sector.
	+ *toezichthouders;* bijvoorbeeld Raden van Toezicht, accountants en de Onderwijsinspectie. Er wordt verwacht dat informatiebeveiliging in de komende jaren een steeds grotere rol gaat spelen bij de goedkeurende verklaring voor de jaarrekeningen van de instellingen. Dat betekent dat ook externe accountants steeds vaker hierover vragen gaan stellen en dat de behoefte aan standaardisatie en normering groot is.
	+ *systeemleveranciers;* instellingen zullen met hun (software) leveranciers, bijvoorbeeld van elektronische leeromgevingen, educatieve software, registratiesystemen, goede afspraken moeten maken over de beveiliging van deze systemen en daarvan afgeleid de verwerking van de persoonsgebonden gegevens (bewerkersovereenkomsten, certificering van leveranciers).
	+ *adviseurs en consultants;* instellingen hebben soms behoefte aan ondersteuning van externe bureaus bij de implementatie van het beleid of bij het beoordelen van hun situatie op het gebied van informatiebeveiliging. Ook deze partijen hebben behoefte aan duidelijke kaders, daarmee wordt ook voorkomen dat diverse partijen hun eigen kaders hanteren.
* **Maatschappij;** tot slot is de maatschappij een belangrijke stakeholder. Leerlingen, studenten, ouders, maar ook de medewerkers en extern ingehuurde medewerkers moeten en mogen ervan uitgaan dat mbo-instellingen op een veilige manier met hun gegevens omgaan en dat hun privacy wordt gewaarborgd. Ook moet de maatschappij ervan kunnen uitgaan dat de resultaten van alle studie inspanningen ook rechtvaardig en correct worden beoordeeld met certificaten of diploma’s met een maatschappelijke waarde die niet ter discussie staat. Mbo-instellingen kunnen dan met trots een waardige diploma-uitreiking organiseren.

In een brede samenwerking tussen het mbo, saMBO-ICT, de MBO Raad, Kennisnet en SURF is de afgelopen twee jaar, onder leiding van een taskforce, het programma ibp ontwikkeld en uitgevoerd. Met dit programma geeft de mbo-sector een adequaat antwoord op de uitdagingen en krijgen de scholen werkbare normenkaders, handreikingen en tooling om de problematiek op een goede wijze aan te pakken. Hierbij heeft het mbo dankbaar gebruik gemaakt van hetgeen in het hoger onderwijs is ontwikkeld en in een vergelijkbare set van documenten is opgeleverd.

In de aanloop van het programma ibp in het mbo hebben saMBO-ICT en Kennisnet twee zogenaamde ‘Hoe? Zo!’-publicaties gemaakt, waarin alle aspecten van zowel informatiebeveiliging als privacy aan de orde komen. Deze aspecten worden weergegeven in een vraag-en-antwoordopzet vanuit het perspectief van de bestuurder of onderwijsmanager. Dit is dan ook de expliciete doelgroep voor deze publicaties. Doel van de publicaties is bijdragen aan een breder begrip van informatiebeveiliging en privacy bij de managers en bestuurders van de mbo-instellingen.

Het resultaat van het programma ibp zelf is het “framework informatiebeveiliging en privacy in het mbo”. Dit is een complete set aan materialen voor de ibp functionaris binnen een mbo-instelling. Hiermee kan deze op een deels gestandaardiseerde en dus vergelijkbare wijze ibp in de instelling implementeren en objectief beoordelen. Daarnaast heeft een objectieve beoordeling aan de hand van het framework geleid tot een benchmark waarvan de eerste resultaten zijn opgenomen. Daardoor kan een eerste beeld worden gegeven hoe de sector mbo presteert op het terrein van ibp. Binnen bijna elke mbo-instelling (90%) is intussen een collega geschoold die daardoor het framework ook daadwerkelijk kan toepassen. Het framework is op 1 augustus 2016 vastgesteld en in de speciale publicatievorm van deze box ter beschikking gesteld aan alle mbo-instellingen en ondersteunende organisaties.

*Het framework gaat voor een deel uit van de NEN-ISO/IEC 27001 en 27002. Op deze wereldwijd toegepaste normen en standaarden rust auteursrecht. Deze normen zijn niet vrij of gratis beschikbaar, maar moeten worden aangeschaft bij NEN. Dit betekent dat bij het gebruik van het framework IBP in het mbo, iedere onderwijsinstelling geacht wordt zelf een toereikende licentie aan te schaffen voor deze normen.*

# Framework informatiebeveiliging en privacy in het mbo

Het ‘framework ibp in het mbo’ bevat alle documenten die voor het mbo ontwikkeld zijn om de implementatie van ibp in het mbo makkelijker te maken. Deze documenten zijn daarin als een soort encyclopedie samengebracht. Uiteraard is het een dynamische boekenkast die voorlopig volop in ontwikkeling blijft. Niet zozeer wat betreft de kaders maar vooral wat betreft de handreikingen, voorbeelden en modellen.



## Onderdelen van het framework

De voornaamste onderdelen van het framework zijn de normenkaders en toetsingskaders. Ter ondersteuning zijn er ook handreikingen, een roadmap, architectuur documenten, data classificatie voorbeelden en nog veel meer.

### Normenkaders

Om te beoordelen of een mbo-instelling informatiebeveiliging en privacy goed op orde heeft, moeten afspraken meetbaar zijn. Het mbo heeft daarom in overleg met alle stakeholders besloten om een normenkader (**Waar wil of moet ik aan voldoen?)** te gaan hanteren voor de informatiebeveiliging.

Belangrijk uitgangspunt is dat deze norm aansluit bij andere gekozen standaarden en voldoet aan internationale normen. Daarom heeft het mbo, net als het hoger onderwijs, besloten om het normenkader ISO 27001 en 27002 te gaan gebruiken. Internationaal is dit een breed gehanteerd normenkader dat door Gartner ook nog eens specifiek voor het mbo is bevestigd.

Op basis van het ISO-kader is een selectie gemaakt van normen die voor het onderwijs relevant zijn. Uit de complete set van 114 normen van de versie 2013 van het ISO 27002 normenkader is een selectie gemaakt van 79 normen, door-vertaald naar 85 statements. De statements zijn in een zestal voor het onderwijs relevante clusters verdeeld:

1. beleid en organisatie;
2. personeel en studenten;
3. ruimten en apparatuur;
4. continuïteit;
5. toegangsbeveiliging en integriteit;
6. controle en logging.

Binnen de mbo-instellingen spelen ook andere zaken die een belangrijke relatie hebben met informatiebeveiliging. De eerste die daarbij opkomt is de bescherming van persoonsgegevens, de privacy wetgeving. Privacy is zeker niet hetzelfde als informatiebeveiliging maar er is wel een grote overlap. Zonder informatiebeveiliging is er geen sprake van privacy.

Voor privacy is echter geen normenkader zoals ISO 27001 en 27002 voorhanden. Daarom is uit de bestaande wet- en regelgeving een aparte set van normen gedestilleerd die voor het onderwijs van belang is en toepasbaar zijn. Deze zijn overzichtelijk samengebracht in een set van regels waar scholen zich aan moeten houden, het zogenaamde ‘compliance kader privacy’. Ten aanzien van privacy is het compliance kader en het toetsingskader geheel up-to-date in relatie tot de nieuwe Europese wetgeving, de Algemene Verordening Privacy (AVG) die de Europese Commissie eind mei 2016 heeft gepubliceerd.

Ook op het gebied van examinering is er een belangrijke overlap met informatiebeveiliging, en ook daarvoor is een dergelijk kader opgesteld. Deels is dit normenkader overlappend met het ISO-kader voor informatiebeveiliging waarbij er is sprake van een gemeenschappelijk deel. Niettemin is het noodzakelijk om aanvullende normen en statements te formuleren om de privacy te waarborgen en om examinering veilig en correct te laten verlopen in een instelling.

Recent is ook digitaal ondertekenen opgenomen in het framework als voorbeeld van een complex proces waarvoor hele goede afspraken op het gebied van informatiebeveiliging moeten worden gemaakt.

In de toekomst is het denkbaar dat ook andere processen een aanvullend kader behoeven.

### Toetsingskaders

Vervolgens zijn bij de normen ook de maatregelen beschreven om deze norm te bereiken en om deze vervolgens ook aan te kunnen tonen (bewijslast). Dit gebeurt in de vorm van een 5-puntenschaal, de zogenaamde ‘maturity levels’. Op basis van deze 5-puntenschaal kan het onderwijs een norm dus op een steeds hoger niveau proberen te realiseren. Bovendien is het normenkader objectief toetsbaar. Met andere woorden: het normenkader wordt een toetsingskader.

Niveau 1 is daarbij het basisniveau. Dit biedt weinig garantie dat het in de norm beschreven risico daadwerkelijk afgedekt wordt. Niveau 5 is het hoogst haalbare maar is vaak niet realistisch. Voor een startende instelling is streefniveau 2 al een hele opgave en is niveau 3 een forse uitdaging. In de afspraken wordt meestal aangegeven wat het minimumniveau moet zijn en wat het streefniveau kan zijn.

Op deze manier ontstaat een geheel dat we het ibp toetsingskader noemen. Omdat dit vanuit het ho-model voor het mbo specifiek gemaakt is noemen we dit ook het ‘ibp toetsingskader mbo’ (**Toetsingskader informatiebeveiliging mbo, IBPDOC3)**. Dit toetsingskader vormt het hart van het ibp programma. Hiermee kunnen instellingen daadwerkelijk toetsen of meten of ze aan de normen voldoen en de benodigde maatregelen ook daadwerkelijk hebben gerealiseerd (de assessments).

Net als bij het normenkader voor informatiebeveiliging is vervolgens op basis van het compliance kader privacy een toetsingskader voor privacy (**Toetsingskader privacy mbo, IBPDOC7)** ontwikkeld. Ook is een toetsingskader voor examinering (**Toetsingskader examinering mbo, IBPDOC8)** ontwikkeld. En daarmee is een set van aanvullende maatregelen beschikbaar om deze thema’s ook op juiste wijze te behandelen, te beveiligen en te toetsen en daarmee te voldoen aan de wet- en regelgeving. Tot slot is er medio 2016 een toetsingskader voor digitaal ondertekenen (**Toetsingskader digitaal ondertekenen mbo, IBPDOC9)** opgeleverd.

### Handreikingen

Vanuit de praktijk is er veel vraag naar praktische handreikingen. Een concreet voorbeeld daarvan is de risico-inventarisatie ibp. Veel instellingen hebben de strategie om risico’s te benoemen en vooral ook te beperken of te vermijden. Vaak wordt dan vanuit de methodiek van risicomanagement een eerste aanpak opgezet. Dit is op zich een goede methodiek, maar het kan heel veel dubbel werk betekenen. In feite is de benadering vanuit het op ISO gebaseerde toetsingskader ook een risico-aanpak.

In de handreiking risico-inventarisatie zijn alle voorkomende risico’s in het mbo al in beeld gebracht en gerelateerd aan de statements in het mbo toetsingskader. Daarmee is een voldoende dekking gerealiseerd om met dit kader de risico’s in het mbo te mitigeren. De belangrijkste risico’s in het mbo zijn op dit moment:

* ongewenste verspreiding van zorgdossiers van leerlingen;
* ongewenste verspreiding van verslagen voortvloeiend uit de gesprekscyclus (functioneren, beoordelen);
* ongecontroleerde toegang tot het netwerk en applicaties;
* verlies van privacy gevoelige data (datalekken);
* verstoring onderwijs en bedrijfsvoering door cybercriminaliteit.

De verschillende toetsingskaders bieden voldoende maatregelen om deze risico’s te beheersen.

# Beheersing, audits en benchmark

Beheersing en ontwikkeling van informatiebeveiliging kan binnen de mbo-sector, in navolging van het hoger onderwijs, opgezet worden als een iteratief proces. Daarbij wordt gebruik gemaakt van de kwaliteitscirkel van Deming (plan-do-check-act). In het framework ibp in het mbo zijn alle relevante documenten voor deze aanpak bijeengebracht. Concreet worden er voor informatiebeveiliging de volgende fasen onderscheiden:

**Fase 1 (plan)**: Uitvoeren **Mbo roadmap informatiebeveiligingsbeleid (IBPDOC5)**.

 Voorwaarde voor fase 1: brede betrokkenheid binnen instellingen: College van Bestuur, ict management, kwaliteitszorg, afdeling HR, juristen en kwartiermaker ibp.

**Fase 2 (do)**: Inrichting beleid aan de hand van het **Model informatiebeveiligings- en privacy beleid voor de mbo-sector (IBPDOC6)**.

 Voorwaarde voor fase 2: actieve betrokkenheid van instellingen met de gebruikersgroep ibp in het mbo, werkgroepen en gezamenlijke projecten (saMBO-ICT en Kennisnet).

**Fase 3 (check):** Toetsing normenkader met een self-assessment, peer review, peer audit, externe audit of benchmark op basis van:

* **Normenkader informatiebeveiliging mbo (IBPDOC2A)** en **Compliance kader privacy (IBPDOC2A)**;
* **Toetsingskader informatiebeveiliging mbo (IBPDOC3)**, ook wel Quick scan genoemd (ook digitaal beschikbaar) en **Toetsingskader privacy mbo (IBPDOC7)**;
* aanvullend **Toetsingskader examinering mbo (IBPDOC8)** en **Toetsingskader digitaal ondertekenen mbo (IBPDOC9).**

 Voorwaarde voor fase 3: aanpak afgestemd met MBO Raad, OCW, externe accountants, externe leveranciers en examencommissies.

**Fase 4 (act):** (jaarlijkse) verbeterplannen

 Voorwaarde voor fase 4: normenkader afgestemd met instellingen, interne en externe auditors.

Naast bovenstaande fasen worden drie niveaus van toetsing onderscheiden:

**Self-assessment** Voor een instelling is het self-assessment een nulmeting met betrekking tot informatiebeveiliging en privacy in de eigen insteling. Daarbij is het niet noodzakelijk om ook echt met procedures en protocollen aan te tonen dat een instelling het beoogde niveau heeft behaald. Bovengenoemde quick scan is hiervoor een hulpmiddel.

**Benchmark** Het is belangrijk om de situatie binnen een instelling te meten op basis van vastgestelde toetsingskader, zodat de instelling weet naar welke onderwerpen vooral aandacht uit moet gaan. Met behulp van een bestaande tool (quick scan) kan de instelling aan het toetsingskader worden afgemeten. De tool maakt het mogelijk om de eigen situatie af te zetten tegen het gemiddelde in de mbo-sector. Dit geeft een duidelijk beeld voor de instelling zelf, maar bij voldoende deelname ook voor de sector als geheel. Daarmee is het een eerste benchmark voor de mbo-sector (nulmeting).

**Peer review** In een peer review controleren instellingen elkaar. Er worden peer-kringen ingericht waarbij instelling A door instelling B wordt gecontroleerd, vervolgens wordt B weer door C gecontroleerd, et cetera. De review wordt als rapport gepresenteerd en beperkt zich tot bevindingen.

**Peer audit** In een peer audit beoordelen instellingen elkaar. Er worden peer-kringen ingericht waarbij instelling A door instelling B wordt beoordeeld, vervolgens wordt B weer door C beoordeeld, et cetera. Resultaten van de audit worden als rapport gepresenteerd en bevatten zowel bevindingen (op basis van document onderzoek, interviews en waarnemingen ter plaatse) als aanbevelingen. Deze kringen zorgen voor een bewustwording bij de beoordeelde en bij de assessor. Het is dus niet alleen een beoordeling, maar is ook onderdeel van het leerproces binnen de mbo-sector.

**Externe audit** Het is de bedoeling om, net als in het hoger onderwijs, het peer audit af te wisselen met externe audits. Dat betekent dat aan een externe partij wordt gevraagd om een audit uit te voeren. Om dit te reguleren en te zorgen dat deze audits op vergelijkbare manier plaatsvinden, zou een gezamenlijke aanbesteding kunnen plaatsvinden voor de instellingen in het mbo. Daarnaast kan het ook een voordeel opleveren in de kosten voor de instellingen zelf.

# Samenwerking en afstemming in het mbo

Samenwerking is van groot belang. Het thema is voor veel instellingen te complex om helemaal zelf aan te pakken. Leren van en met elkaar is noodzakelijk. Als iedereen het wiel moet gaan uitvinden is dat een zware taak. Het gezamenlijke scholingstraject van de masterclasses is een cruciale factor gebleken in de enorme vlucht die de mbo-instellingen met ibp gemaakt hebben. Als ervaringen, ideeën, oplossingen en producten met elkaar gedeeld worden scheelt dat aanzienlijk. Het is vooral cruciaal om samen te werken aan modellen, overeenkomsten en afspraken kaders, zodat de sector in de hele informatie-keten als goede partner effectief en efficiënt kan functioneren.

Daarbij komt nog dat we als onderwijssector hebben afgesproken met OCW om te komen tot zelfregulering. De sector heeft zich tot doel gesteld om informatiebeveiliging en privacy op een adequate wijze zelf te regelen. Dat betekent dat we als sector de ruimte krijgen om het op onze manier te regelen. Maar dit leidt ook tot de verplichting om te laten zien hoe we als sector hierin presteren, Concreet betekent dit dat we als sector afspraken moeten maken over de te hanteren standaarden en de daarin te bereiken ‘baseline’. Aan deze baseline moeten alle instellingen minimaal voldoen. Maar ook over de ambitie. Waar wil het mbo over een bepaalde periode staan op het gebied van ibp? Dat betekent ook transparantie. We moeten met assessments en audits helder in beeld brengen wat de stand van zaken is binnen het mbo is. De benchmark zal hierin een cruciale rol spelen. Pas dan kan de sector met OCW een bindende afspraak maken over de manier waarop ibp in het mbo gestalte krijgt.

De aanzet vanuit saMBO-ICT om een taskforce ibp in het mbo op te richten was de eerste stap tot samenwerking in de mbo-sector. Het mbo-veld heeft heel positief op dit initiatief gereageerd. Dit heeft geleid tot:

* een grote inspanning vanuit de mbo-instellingen om het framework te realiseren (taskforce, werkgroepen, input vanuit de scholingsprogramma’s door de deelnemers);
* veel aandacht voor de publicaties ‘Hoe? Zo! Informatiebeveiligingsbeleid’ en ‘Hoe? Zo! Privacy in het mbo’;
* een hoge mate van participatie in het scholingsprogramma, de masterclasses (basis ibp, privacy, peer review);
* een concrete aanpak van de problematiek in het overgrote deel van de mbo-instellingen (> 90%).

Het programma en de resultaten zijn eind 2015 overgedragen aan een gebruikersgroep ibp in het mbo, onder de vlag van saMBO-ICT. De groep bestaat uit vertegenwoordigers vanuit de instellingen (3 collega’s) en de ondersteunende organisaties Kennisnet en SURF.

In de figuur hiernaast is de structuur van de huidige ibp organisatie in het mbo weergegeven. De gebruikersgroep heeft een netwerk ingericht waarin alle instellingen deelnemen met een contactpersoon, meestal de ibp manager, security officer, privacy officer of functionaris gegevensbescherming. De regie op het hele proces wordt vanuit de gebruikersgroep vormgegeven. Het netwerk zal een cruciale rol spelen bij de uitwisseling van kennis en ervaring tussen de instellingen en bij het faciliteren van de samenwerking tussen de instellingen.

# De praktijk

In de praktijk is het behoorlijk complex om informatiebeveiliging en privacy in te bedden in het mbo. Dat geldt zowel voor de verantwoordelijken als voor de uitvoerders. Ga er maar aan staan. Het blijkt keer op keer in het mbo dat samenwerking en uitwisseling een groot goed is. Het heeft ons zeker in de sfeer van ict ook al veel opgeleverd. Belangrijk is om in dit verantwoordingsdocument ook de praktijk en de urgentie zoals die in de instellingen wordt gevoeld weer te geven. Daarom hebben we aan een voorzitter van een College van Bestuur als eindverantwoordelijke en aan een ibp manager als uitvoerder gevraagd hun ervaringen en ideeën over informatiebeveiliging en privacy zowel in het mbo in het algemeen als in hun eigen instelling in het bijzonder hier te delen.

## Interview met Ben Geerdink.

Ben Geerdink is naast voorzitter van het CvB van het Rijn IJssel College ook voorzitter van het bestuur van saMBO-ICT en heeft hierdoor een heel duidelijk perspectief van de samenwerking van alle mbo-instellingen op dit gebied.

 **“We moeten in het mbo samen de mouwen opstropen”**

De uitgave van het framework informatiebeveiliging en privacy (ibp) benadrukt nog eens hoe belangrijk het is dat ibp op het mbo bestuurlijk wordt ingebed. Ben Geerdink is voorzitter van het college van bestuur van Rijn IJssel. Daarnaast is hij voorzitter van het bestuur van saMBO-ICT en vervult daarmee een belangrijke rol naar de besturen in het mbo.

**Hoe hoog staat informatiebeveiliging op de agenda van Rijn IJssel?**

“Het onderwerp informatiebeveiliging en privacy leeft steeds meer binnen Rijn IJssel. We hadden al een privacyreglement en informatiebeveiliging was altijd goed belegd bij de ict-afdeling. Maar mede door de activiteiten van saMBO-ICT, Kennisnet en SURF zien we nog beter hoe belangrijk aandacht voor ibp is. In huis zijn we er flink mee aan de slag gegaan. We hebben een projectleider benoemd die volgt wat er landelijk gebeurt en dat vertaalt naar activiteiten binnen onze organisatie. Kortom, er is flink beweging maar dat is ook nodig.”

**Wat is jouw rol als voorzitter van het CvB?**

“Het is mijn rol om ibp aan te jagen en er voldoende aandacht voor te vragen bij de medewerkers en het management. Voortdurend wordt het CvB bestookt met actuele ontwikkelingen die allemaal aandacht verdienen. Het is de kunst om ervoor te zorgen dat onze aandacht over al deze onderwerpen gelijkwaardig wordt verdeeld.”

**Waarom is het zo belangrijk om ibp binnen het mbo samen aan te pakken?**

**“**Het onderwerp informatiebeveiliging en privacy is van belang voor de hele mbo-sector. Het is daarom essentieel dat we bij anderen kijken en van elkaar leren. Die kracht benutten we in het mbo vaak. We gebruiken elkaars kennis in plaats van dat we allemaal zelf opnieuw het wiel uitvinden. Samen stropen we de mouwen op en maken we oplossingen concreet. De complexiteit van dit onderwerp dwingt ons daar ook toe.”

**Is de mbo-sector helemaal zelf verantwoordelijk voor de aanpak van ibp?**

“De sector heeft met het ministerie van Onderwijs, Cultuur en Wetenschap (OCW) gekozen voor zelfregulering. En dat helpt ons heel goed. Het werkt vaak beter als je zelf de regie voert dan als je van bovenaf zaken krijgt opgelegd. We kunnen nu in het mbo in ons eigen tempo veranderingen doorvoeren die aansluiten bij onze organisatie. Natuurlijk moeten we wel evalueren of deze veranderingen voldoende zijn en erop toezien dat er echt iets gebeurt. Zelfregulering mag absoluut geen excuus zijn om niks te doen of veranderingen uit te stellen.”

**Heb je nog een persoonlijk advies voor collega’s?**

“Ik zou mijn collega’s willen meegeven om het onderwerp informatiebeveiliging voldoende aandacht te geven. Niks doen is een groot risico, want er gaat ongetwijfeld een keer iets mis. Het is dan belangrijk dat je als instelling een helder en transparant verhaal hebt, gebaseerd op een gedegen werkplan. Wat heb je gedaan om de risico’s te verminderen? Niet alleen voor je eigen instelling, maar voor de hele sector. Daarmee laten we als sector zien dat we informatiebeveiliging aandacht geven en dat we dus *in control* zijn.”

## Interview met Martien van Beekveld

Martien van Beekveld is verantwoordelijk voor de implementatie van ibp in het Summa College in Eindhoven, een mbo-instelling die er al een aantal jaren aan werkt om ibp binnen de school vorm te geven.

 **“Informatiebeveiliging moet dagelijkse routine worden”**

Martien van Beekveld is manager informatiebeveiliging en privacy (ibp) bij het Summa College. Ook is hij vertegenwoordiger van de instellingen in de kerngroep van de gebruikersgroep ibp van saMBO-ICT, SURF en Kennisnet. We vroegen hem naar de aanpak van het Summa College en zijn rol als ibp’er daarin.

**Hoe leeft informatiebeveiliging en privacy binnen het Summa College?**

“Bij het Summa College nemen we ibp heel serieus. Uit de eerste MBO IB-audit van begin 2016 bleek dat het Summa College een volwassenheidsniveau heeft van 2.0. Dit houdt in dat op dit moment een relatief klein deel van onze organisatie bekend is met informatiebeveiliging en privacy. Er valt dus nog veel te verbeteren. Daarom ben ik in mei 2015 aangesteld als ibp-manager. In de tweede helft van 2015 hebben we onder meer een ibp-roadmap gemaakt en een verbeterplan opgesteld voor de periode 2015-2019.”

**Wat betekent het voor jou om ibp-manager binnen een mbo-instelling te zijn?**

“Ik help het Summa College om het geformuleerde ibp-beleid te implementeren. Dat is een serieuze uitdaging. Mijn collega’s hebben al zo veel op hun bord, en dan komt er ook nog een of andere ibp’er die nog meer van ze wil. Ook merk ik dat veel collega’s denken dat ibp heel complex en niet vanzelfsprekend is. Het is mijn taak om ze ervan te overtuigen dat ibp geen extra werk is, maar onderdeel moet worden van de dagelijkse routine.”

**Wat zijn de belangrijkste succesfactoren voor een goede implementatie van ibp?**

“De belangrijkste succesfactor is steun van het CvB en management én van de werkvloer. Anders kom je er niet. Je moet het echt samen doen. Maak daarnaast handig gebruik van de documenten in het framework ibp voor het mbo, zoals de roadmap waarop je je eigen ibp-roadmap kunt baseren. En stel daarnaast een ibp’er aan die de rol van ambassadeur op zich neemt, zonder voor politieagent te gaan spelen. Pak de aanpak van ibp serieus aan, het is niet iets om er zomaar even bij te doen.”

**Welke belangrijke knelpunten of valkuilen kom je tegen?**

“Allereerst denken veel collega’s dus dat ibp heel veel moeite kost. Zeker bovenop de hoge werkdruk die er binnen de organisatie al is. Daarnaast rust er vaak een taboe op ibp-incidenten. Als er iets gebeurt, wordt dat in veel gevallen onder de pet gehouden. Terwijl een incident juist een leermoment moet zijn voor de hele organisatie.”

**Wat is het belang van de gebruikersgroep ibp voor het mbo?**

“We moeten continu het ibp-kennisniveau blijven verbeteren, bijvoorbeeld door het organiseren van masterclasses en expertsessies. Daarnaast is het belangrijk dat mbo-instellingen samen optrekken en leren van elkaars ervaringen. We staan er niet alleen voor! Ook van de aanpak in het hoger onderwijs, primair en voortgezet onderwijs kunnen we leren. We moeten daarom ook regelmatig kennis uitwisselen met collega’s in deze sectoren.”

**Welk advies heb je voor collega’s die nog met ibp aan de slag moeten?**

“Ga ervoor! Geef ibp de aandacht die het nodig heeft en maak collega’s bewust van de noodzaak ervan. Start met de aanpak van laaghangend fruit, zoals het versleutelen van alle laptops binnen de organisatie. Maar ontwikkel ook een roadmap voor de lange termijn en deel die met alle organisatieonderdelen. En tot slot: maak handig gebruik van alle kennis en ervaring binnen de gebruikersgroep ibp.”

Overzicht framework

**Documenten en publicaties framework ibp in het mbo, 1/8/2016**

**Nummer omschrijving**

* IBPDOC1 Verantwoordingsdocument informatiebeveiliging en privacy in het mbo onderwijs
* [IBPDOC2A Normenkader informatiebeveiliging mbo](https://groepen.sambo-ict.nl/file/download/12372)
* IBPDOC2B Privacy compliance kader mbo
* [IBPDOC3 Toetsingskader informatiebeveiliging: clusters 1 t/m 6](https://groepen.sambo-ict.nl/file/download/12373)
* IBPDOC4 Mbo ibp architectuur
* IBPDOC5 Mbo roadmap informatiebeveiligings- en privacy beleid
* IBPDOC6 Model informatiebeveiligings- en privacy beleid voor de mbo sector
* IBPDOC7 Toetsingskader privacy: cluster 7
* IBPDOC8 Toetsingskader examinering pluscluster 8
* IBPDOC9 Toetsingskader digitaal ondertekenen pluscluster 9
* IBPDOC10 Toetsingskader vmbo-mbo pluscluster 10 (nog in ontwikkeling)
* [IBPDOC11 Benchmark mbo sector](https://groepen.sambo-ict.nl/file/download/12374)
* IBPDOC12 Functiewaardering ibp
* IBPDOC13 Positionering ibp
* IBPDOC14 Handleiding BIV classificatie
* IBPDOC15 BIV en PIA bekostiging
* IBPDOC16 BIV en PIA indiensttreding
* IBPDOC17 BIV en PIA online leren
* [IBPDOC18 Bewerkersovereenkomst mbo versie](https://groepen.sambo-ict.nl/file/download/12381)
* IBPDOC19 Certificeringsschema ibp ROSA
* IBPDOC20 Format Dataregister
* IBPDOC21 Handboek normenkader ib, compliance kader privacy en normenkader examineren
* [IBPDOC22 Handleiding](https://groepen.sambo-ict.nl/file/download/12375) Privacy by Desigg
* [IBPDOC23 Autorisatie](https://groepen.sambo-ict.nl/file/download/12376) Architectuur
* [IBPDOC24 Starterkit bcm mbo versie](https://groepen.sambo-ict.nl/file/download/12377)
* [IBPDOC25 Integriteit code mbo versie](https://groepen.sambo-ict.nl/file/download/12378)
* [IBPDOC26 Verantwoord](https://groepen.sambo-ict.nl/file/download/12379) network gebruik
* [IBPDOC27 Responsible disclosure mbo versie](https://groepen.sambo-ict.nl/file/download/12380)
* [IBPDOC28 Bewerkersovereenkomst mbo versie](https://groepen.sambo-ict.nl/file/download/12381)
* [IBPDOC29 Risico inventarisatie ibp](https://groepen.sambo-ict.nl/file/download/12382)
* [IBPDOC30 Technische quick scan (APK)](https://groepen.sambo-ict.nl/file/download/12383)

**Andere producten:**

* [Programma Informatiebeveiliging 2015](https://www.sambo-ict.nl/wp-content/uploads/2015/02/Folder-informatiebeveiliging-2015-V2.pdf)
* [Hoe? Zo! Informatiebeveiligingsbeleid in het mbo](https://www.sambo-ict.nl/wp-content/uploads/2014/09/KNS_Informatiebeveiliging_FINAL4A.pdf)
* [Hoe? Zo! Privacy in het mbo](https://www.kennisnet.nl/fileadmin/kennisnet/publicatie/hoezo/Hoe_Zo_Privacy_in_het_mbo.pdf)