APS IT diensten

Voor ICT in het belang van je school

Een digitaal veilige school

Aan de slag met het normenkader IBP

Even kennismaken

- Tonny Plas, directeur Privacy op School
- Menno Smidts, directeur APS IT Diensten

APS IT diensten

Voor ICT in het belang van je school

Inhoud

1. Wat moet je weten over het Normenkader IBP?
2. Hoe ga je aan de slag?
3. Wat kunnen Privacy op School en APS IT Diensten samen betekenen?

APS IT diensten

Voor ICT in het belang van je school

1. Wat moet je weten?

PRIVACY OP SCHOOL

APS IT diensten
Voor ICT in het belang van je school

Opbouw en doel Normenkader

- Beschrijvende normen voor IB&P met praktische voorbeeldmaatregelen
- Afgeleide van het bestaande kader in HBO en WO → NBA Volwassenheidsmodel voor Informatiebeveiliging
- 15 domeinen en 69 normen voor Informatiebeveiliging
- Je moet van elke norm de werking kunnen aantonen
- 1 domein voor Privacy (deze wordt begin juni verwacht)
- **Eind 2027** dient elke school hier aan te voldoen (verplichting!)

''Een onderwijssector waarin iedere leerling digitaal veilig kan leren en medewerkers digitaal veilig kunnen werken''

PRIVACY OP SCHOOL

APS IT diensten
Voor ICT in het belang van je school

Normenkader Privacy

1. Beleid (BL):

- Privacy beleid
- Rollen, taken en verantwoordelijkheden
- Risico's

2. Processen (PR)

- Operationele processen
- Verwerkingsregister opzet en vastlegging verwerkingen
- Verwerkingsregister actualisatie
- Identificatie van risico's (met behulp van pre-DPIA's)
- DPIA's
- Gegevensbescherming door ontwerp en standaardinstellingen (Privacy by Design & Privacy by Default)
- Bewaar- en vernietigingsbeleid

3. Organieke inbedding (OI)

- Aanwijzing en positie FG
- Privacyorganisatie
- Betrokkenheid medezeggenschap
- Bewustwording

4. Rechten van betrokkenen (RB)

- Afhandeling rechten van betrokkenen
- Informatieplicht
- Toestemming
- Geautomatiseerde individuele besluitvorming waaronder profilering

5. Samenwerking (SW)

- AVG-rollen
- Toetsing gegevensverstrekking aan derden
- Doorgifte buiten de EER

6. Beveiliging (GB)

- Datalekken detectie, classificatie en afhandeling
- Melding van datalekken aan AP en betrokkenen
- Informatiebeveiliging (Normenkader deel 1)

7. Verantwoording VW)

- Rapportage

Volwassenheidsniveaus

Omschrijving volwassenheidsniveau		Toelichting
1	Maatregelen zijn **ad hoc**	Beheersmaatregelen zijn niet of slechts gedeeltelijk vastgesteld en/of worden op een inconsistente manier uitgevoerd en zijn sterk afhankelijk van individuen.
2	Maatregelen **bestaan** en worden op consistente wijze uitgevoerd	Beheersmaatregelen bestaan en worden op een gestructureerde en consistente, maar informele manier uitgevoerd.
3	Maatregelen zijn gedocumenteerd en de uitvoering is in **werking**	Beheersmaatregelen zijn gedocumenteerd en worden op een gestructureerde en formele manier uitgevoerd. Uitvoering van de maatregelen is aantoonbaar, getest en effectief.
4	Er is een **verbetercyclus** aanwezig en gedocumenteerd	De effectiviteit van beheersmaatregelen wordt periodiek beoordeeld en indien nodig verbeterd. Deze beoordeling is gedocumenteerd.
5	Er is een **bedrijfsbrede aanpak** van risico's	Een bedrijfsbreed risico- en beheersprogramma voorziet in continue en effectieve beheersing en aanpak van risico's.

BASELINE

Beleid moet dus op papier gezet worden en uitgevoerd worden door het nemen van:

- technische maatregelen
- juridische maatregelen
- organisatorische maatregelen

PRIVACY OP SCHOOL

Wat moet je aan kunnen tonen?

APS IT diensten
Voor ICT in het belang van je school

1. ☐ **Visie & Strategie [vastgesteld] – 1.1**
2. ☐ **IBP-beleid [goedgekeurd] -1.2**
3. ☐ **Jaarlijkse aandacht voor IBP - 1.2**
4. ☐ **Onboardingproces – 1.2**
5. ☐ **Procurementproces; IBP-beleid onderdeel van inkoop eisen - 1.2**
6. ☐ **Informatiebeveiligingsplan (Planning/Roadmap) [goedgekeurd] - 1.3**
7. ☐ **Jaarrapportage planning/roadmap - 1.3**
8. ☐ **Functiebeschrijving; informatiemanagement en architectuur in functiepakket benoemd – 1.4**
9. ☐ Referentie Architectuur = FORA [vastgesteld] - 1.4
10. ☐ EIAM [goedgekeurd] – 1.4
11. ☐ **Auditplan beleid – 1.5**
12. ☐ Auditplan uitvoering [goedgekeurd] – 1.5
13. ☐ Auditcommisie; wie zijn lid van het team – 1.5
14. ☐ Checklists – 1.5
15. ☐ Auditrapport – 1.5
16. ☐ Actieplan n.a.v. auditrapport – 1.5
17. ☐ **Rollen, verantwoordelijkheden (aansprakelijkheid) en governancestructuur – 2**
18. ☐ **Intentieverklaring – 2.1**
19. ☐ **Autorisatiematrix beleid – 2.2**
20. ☐ Toezicht bij afwijking van richtlijn logische toegangsbeveiliging – 2.2
21. ☐ **Autorisatiematrix [vastgesteld] – 2.2**
22. ☐ **Informatierisicomanagementbeleid – 3.1**
23. ☐ **Informatierisicomanagementproces [goedgekeurd] – 3.1**
24. ☐ Bedrijfsdoelstellingen – 3.2
25. ☐ Risicomanagementproces – 3.2
26. ☐ **Risicoanalyses – 3.2**

...

126. ☐ Proces voor back-up en herstel van systemen, applicaties, data en documentatie – 13.2
127. ☐ Dataherstel opgenomen in BCP (norm 14.1) – 13.2
128. ☐ Beleid Capacity & Performance management – 13.3
129. ☐ Proces Capacity & Performance management – 13.3
130. ☐ **Bedrijfscontinuïteitsmanagement beleid – 14.1**
131. ☐ Bedrijfs- & IT-continuïteitsplan [vastgesteld] – 14.1
132. ☐ Bedrijfscontinuïteitsplan test – 14.2
133. ☐ Rapportage bedrijfscontinuïteitsplan test 14.2
134. ☐ Proces off-site back-up opslag [vastgesteld/goedgekeurd] -14.3
135. ☐ Proces voor datareplicatie – 14.4
136. ☐ **Crisismanagementplan - 14.5**
137. ☐ **Proces voor Crisisoefening – 14.5**
138. ☐ **Beleid ketenbeheer – 15.1**
139. ☐ **Proces voor inkoop van IT services – 15.1**
140. ☐ Standaard SLA [goedgekeurd] – 15.1
141. ☐ Proces Leveranciersmanagement - sub Service Level Management [goedgekeurd] – 15.2
142. ☐ Rapportage SLA beoordeling – 15.2
143. ☐ Proces Leveranciersmanagement - sub leveranciersrisicomanagement [goedgekeurd] – 15.3
144. ☐ Leveranciersmanagement risicoanalyse – 15.3
145. ☐ Proces Leveranciersmanagement - sub Toetsing van Interne Beheersmaatregelen [goedgekeurd] -15.4

PRIVACY OP SCHOOL

APS IT diensten
Voor ICT in het belang van je school

Groeipad?

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
De basis op orde	1.1 1.2	2.1				6.1 6.2 6.4	7.1 7.2 7.3		9.1 9.2 9.3			12.1		14.1 14.5	
Mitigeren *hoge* risico's			3.2 3.3	4.6			7.4 7.5 7.6	8.1 8.2	9.5	10.1 10.2 10.3 10.5	11.12 11.13	12.2	13.2	14.2 14.3	15.3
Mitigeren *medium* risico's	1.4 1.5	2.2			5.1	6.3			9.4 9.6		11.1 11.3 11.5 11.7		13.3	14.4	15.1 15.2 15.4
Verdere verfijning	1.3			4.2 4.3 4.5				8.3		10.4	11.8 11.9 11.10 11.11		13.1		

2. Hoe ga je aan de slag?

PRIVACY OP SCHOOL

APS IT diensten
Voor ICT in het belang van je school

Wijs eigenaren aan

Domein	Primaire Eigenaar(s)	Secundaire Eigenaar(s)
01 Bestuur	CvB	PO
02 Organisatie	CvB	PO
03 Risicomanagement	CvB, PO, CISO	ICT
04 Personeelsbeheer	HRM	ICT
05 Configuration Management	ICT	
06 Incident/Problem Management	ICT, CISO	PO
07 Change Management	ICT	
08 Systeemontwikkeling	ICT	
09 Datamanagement	HRM, Onderwijs	ICT, PO
10 Identity & Access Management	HRM	ICT
11 Security Management	CISO	ICT, HR, Onderwijs
12 Fysieke beveiliging	FM	ICT, CISO
13 IT-operatie	IT	CISO
14 Bedrijfscontinuïteits management	CvB	ICT
15 Ketenbeheer	Inkoop	ICT

PRIVACY OP SCHOOL

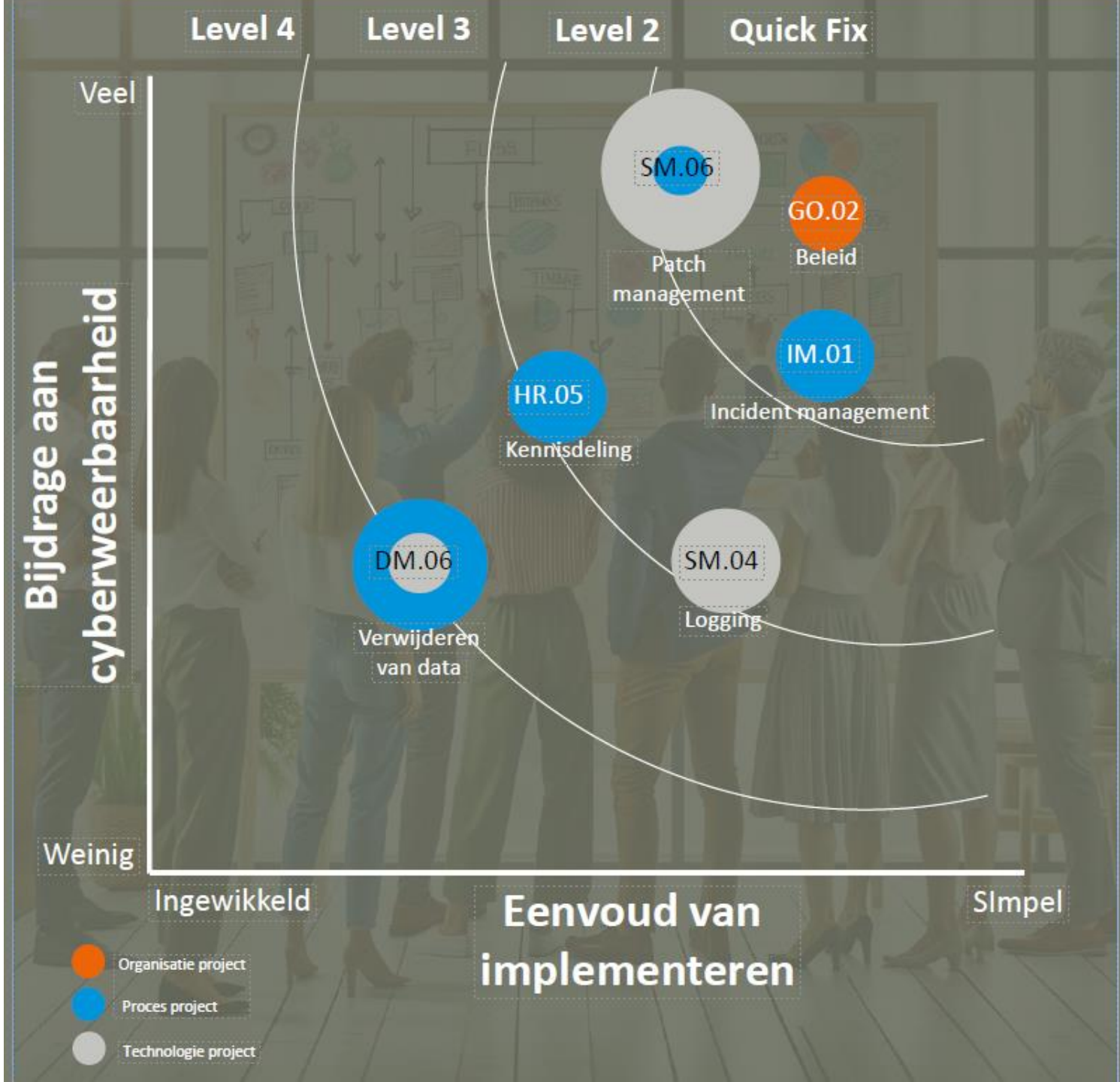
Breng jouw bestuur in kaart!

APS IT diensten
Voor ICT in het belang van je school

1.	Bestuur (Governance; GO)	~1,0	
2.	Organisation (OR)	~1,0	
3.	Risicomanagement (RM)	~1,0	
4.	Personeelsbeheer (HR)	~1,7	
5.	Configuration Management (CO)	~1,0	
6.	Incident/problem management (IM)	~1,5	
7.	Change management (CH)	~1,8	
8.	Systeemontwikkeling (SD)	~1,0	
9.	Datamanagement (DM)	~1,3	
10.	Identity & Access Management (ID)	~2,6	
11.	Security Management (SM)	~1,5	
12.	Fysieke beveiliging (PH)	~1,5	
13.	IT-operatie (OP)	~3,0	
14.	Bedrijfscontinuïteitsmanagement (BC)	~1,0	
15.	Ketenbeheer (SC)	~1,0	

PRIVACY OP SCHOOL

Begin met high impact en low fruit



Kelvin Rorive, 2024

PRIVACY OP SCHOOL

APS IT diensten
Voor ICT in het belang van je school

Werk gefaseerd

Kelvin Rorive, 2024

PRIVACY OP SCHOOL

APS IT diensten
Voor ICT in het belang van je school

Werk risicogebaseerd

Denk als een hacker
Zorg voor onaantrekkelijke hack-omgeving

Meest voorkomende zwaktes:

- Admin wachtwoorden simpel en onveilig opgeslagen
- Onbeheerde kwetsbare systemen
- Zwakke hardware beveiliging
- Te veel rechten aan gebruikers en admins

Gebruik dezelfde tools als hackers:

- Kwetsbaarheden scans
- Breach & Attack Services

Kelvin Rorive, 2024


Verkrijgen initiële toegang
Consolideren positie
Wegsluizen informatie
Inzetten ransomware
Financiële afhandeling

NCSC

PRIVACY OP SCHOOL

Werk samen in jouw regio!

Formuleer een visie

Kelvin Rorive, 2024

3. Hoe kunnen we jou helpen?

11 basismaatregelen

“Met deze basismaatregelen zet je eerste concrete stappen om jouw school digitaal veiliger te maken.”

De basismaatregelen zijn geïnspireerd door publicaties van het Nationaal Cyber Security Centrum (NCSC), het Digital Trust Center. De maatregelen worden aangeraden door het programma Digitaal Veilig Onderwijs.

1. Breng je applicaties en omgevingen in kaart
2. Maak afspraken met leveranciers
3. Richt risicomanagement in
4. Bepaal wie toegang heeft tot je data en diensten en leg uit waarom personen toegang moeten hebben
5. Beperk het aanvalsoppervlak
6. Versleutel opslagmedia met gevoelige bedrijfsinformatie en privacygevoelige gegevens
7. Bescherm je organisatie tegen het verlies van gegevens door regelmatig back-ups te maken en te testen
8. Gebruik antivirus-software
9. Pas multifactorauthenticatie toe op de kritieke systemen
10. Centraliseer en analyseer loginformatie
11. Installeer tijdig en op een gestructureerde manier updates

Basismaatregel 1

Breng je applicaties en omgevingen in kaart en eigenaren en richt een proces in als het fout gaat

Deze maatregel heeft een relatie met de normen: 2.1 | 5.2 | 9.1 | 14.1 | 14.2 | 15.3

- Breng je applicatie in kaart en je datastromen (verwerkingsregister, Microsoft Cloud App Security)
- Maak een noodplan

De eerste stap naar veilige digitaal onderwijs: Wijs proceseigenaren aan en classificeer de gegevens in jouw school

Ondewijsevaluatie	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Beleid en planning	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Verantwoording	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Medezeggenschap	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Visie en governance	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Verantwoording	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Onderwijsvoorbereiding	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Real. onderhoud en dig. toeg.heid	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Samenwerking en comm. mw. ext.	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Ouderbetrokkenheid ouder-school	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Veiligheidswaarborging	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Medezeggenschap	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Onderwijs-uitvoering	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Beschikbaarheid		
Hoe lang mag data niet beschikbaar zijn?		
L = > 7 dagen	M = > 1-6 dgn	H = < 1dag

Integriteit		
Hoe erg is het als data niet juist of actueel is?		
L = niet erg	M = enigszins	H = heel erg

Vertrouwelijkheid		
Voor wie mag de data toegankelijk zijn?		
L = > onbep.	M = spec. grp.	H = spec. rol.

Leerlingbegeleiding	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Strategie en beleid	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

In-, door- en uitstroom	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Organisatie passend onderwijs	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Klachten en bezwaren	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Fac. leerlingcommunicatie	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Zorgbegeleiding en communicatie	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

...	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Fac. oudercommunicatie	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Juridische zaken	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Personeel en organisatie	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Financieel beheer en bekostiging	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Informatiemanagement	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

...	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Facilitair beheer	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Inkoop en contractbeheer	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

Informatiebeveiliging en privacy	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

PR en communicatie	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

ICT-ondersteuning	
<eigenaar>	<naam systeem>
Classificatie:	B-I-V
RA / DPIA*:	VWO: Ja/Nee*

COLOFON	
Naam invuller	
Datum bijgewerkt:	
Versie:	

* Streep door wat niet van toepassing is

APS IT diensten
Voor ICT in het belang van je school

Basismaatregel 2

Maak afspraken met leveranciers

Deze maatregel heeft een relatie met de normen: 15.1 | 15.2 | 15.3 |15.4

- Laat je verwerkersovereenkomsten beoordelen
- Vraag om ISO 27001 / SOC type 2 verklaring

Basismaatregel 3

Richt risicomanagement in

Deze maatregel heeft een relatie met de normen: 3.1 | 3.2 | 3.3

- Stel risicomanagementbeleid op
- Voer risicoanalyses uit
- Voer DPIA’s uit
- Voer een Protect 365 – data security assessement uit

APS IT diensten
Voor ICT in het belang van je school

Basismaatregel 4

Bepaal wie toegang heeft tot je data en diensten en leg uit waarom personen toegang moeten hebben

Deze maatregel heeft een relatie met de normen: 4.4 | 10.1 | 10.2 | 10.5

- Stel toegangsbeveiligingsbeleid (IAM) op
- Stel autorisatiematrices vast

Aan de slag!

Beperk het aanvalsoppervlak

Deze maatregel heeft een relatie met de normen: 11.1 | 11.11 | 11.12

- Voer een APK uit op Microsoft 365
- Voer kwetsbaarhedenscans en pentesten uit
- Netwerksegmentering
- Zorg voor global admin accounts die niet extern beschikbaar zijn (global admin met beperkte rechten)

APS IT diensten
Voor ICT in het belang van je school

Basismaatregel 5

Versleutel opslagmedia met gevoelige bedrijfsinformatie van belangrijke bedrijfsgegevens en privacygevoelige gegevens

Deze maatregel heeft een relatie met de normen: 9.3 | 9.4 | 11.3

- Richt je MDM goed in
- Volg de Intune basistraining
- Gebruik Bitlocker / versleuteling

APS IT diensten
Voor ICT in het belang van je school

Basismaatregel 7

Bescherm je organisatie tegen het verlies van gegevens door regelmatig back-ups te maken en te testen

Deze maatregel heeft een relatie met de normen: 13.1 | 13.2 | 14.3

- Maak een backup van je kroonjuwelen
- Test je backup

APS IT diensten
Voor ICT in het belang van je school

Basismaatregel 8

Gebruik antivirus-software

Deze maatregel heeft een relatie met de normen: 11.12

- Maak gebruik van beheerde devices
- Configureer Windows Defender

APS IT diensten
Voor ICT in het belang van je school

Basismaatregel 9

Pas multifactorauthenticatie toe op de kritieke systemen

Deze maatregel heeft een relatie met de normen: 11.12

- Gebruik MFA
- Gebruik een wachtwoordmanager

APS IT diensten
Voor ICT in het belang van je school

Basismaatregel 10

Centraliseer en analyseer loginformatie

Deze maatregel heeft een relatie met de normen: 10.1 | 10.4

- Bespreek dit onderwerp met je cloudleveranciers
- Richt hiervoor processen in

Basismaatregel 11

Installeer tijdig en op een gestructureerde manier updates

Deze maatregel heeft een relatie met de normen: 5.2

- Bespreek dit met je leverancier
- Zorg voor goede afspraken (patchmanagement)
- Neem een pentest af

Samenwerking Privacy op School en APS IT

- Kennis van het onderwijs in combinatie met ICT en IBP
- Opleider op het gebied van IBP in het onderwijs
  - Kijk op https://www.apsitdiensten.nl/trainingen-overzicht
- Aanbod op het gebied van IBP voor scholen in het PO
  - Kijk op https://www.privacyopschool.nl/bewustwording-webshop/

Kom naar de informatiebijeenkomst:
Op weg naar het normenkader IBP

Zwolle (bij OOZ) – donderdag 23 mei van 9.00 tot 13.00 uur

Tilburg (bij Biezonderwijs) – maandag 3 juni van 12.30 tot 17.00 uur

Utrecht (bij APS IT-diensten) – dinsdag 11 juni van 12.30 tot 17.00 uur

APS IT diensten

Voor ICT in het belang van je school

APS IT-diensten
Zwarte Woud 2
3524 SJ Utrecht

www.apsitdiensten.nl

T 030 2856 870
M info@apsitdiensten.nl