ossewold.net
KENNIS • PASSIE • GROEI

Normenkader IBP FO

samen op weg naar digitale veiligheid

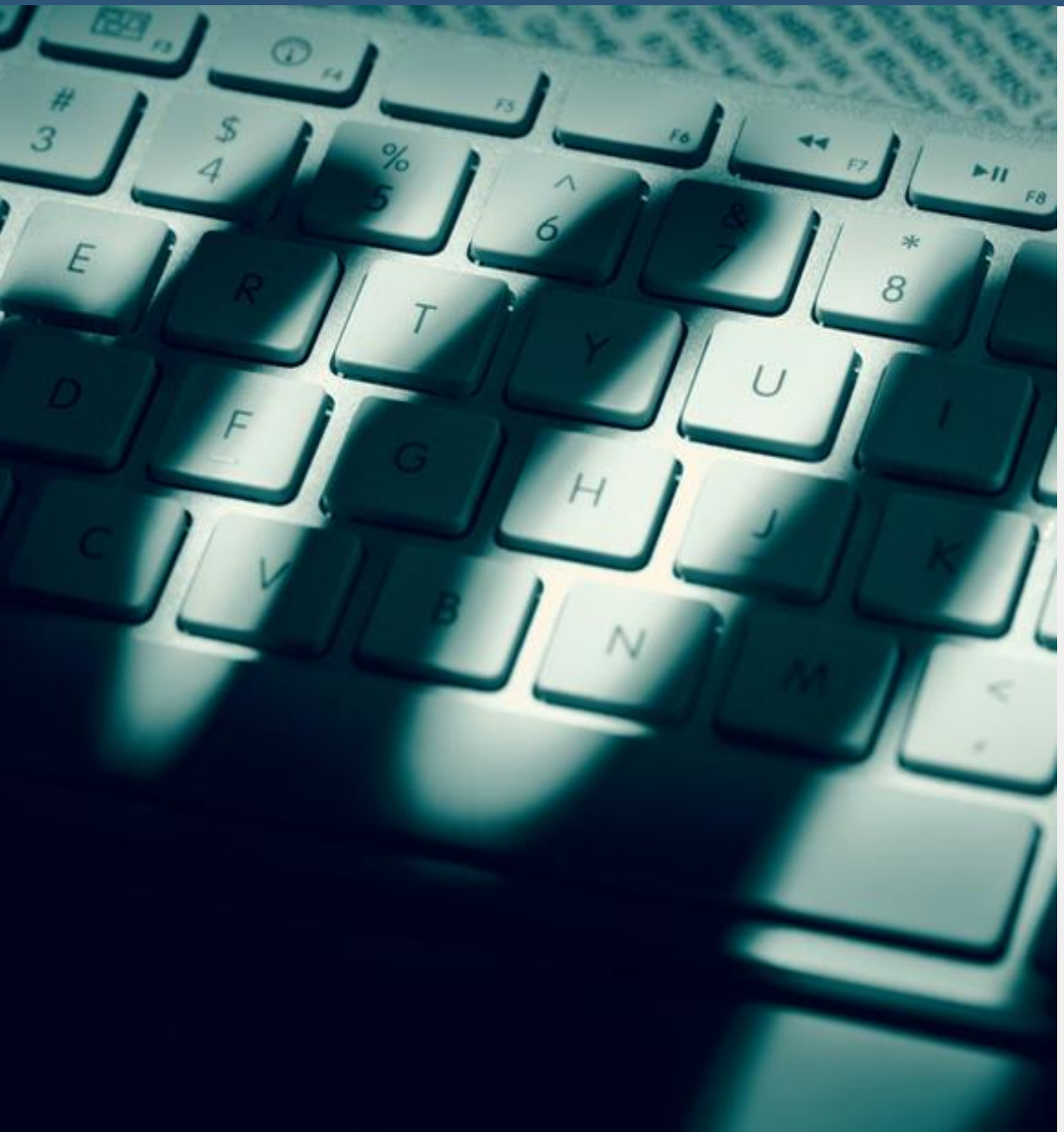
Normenkader IBP FO

Vanaf 2025 moet in het jaarverslag aandacht besteed worden aan de uitvoering van het Informatiebeveiliging- en Privacy beleid.

Het Normenkader Informatiebeveiliging en Privacy voor Funderend onderwijs (IBP FO) beschrijft de normen voor een digitaal veilige schoolorganisatie en biedt concrete voorbeeldmaatregelen voor schoolbesturen.

Op dit moment is het normenkader nog niet juridisch verplicht. Naar verwachting is dat in 2027 wel het geval. Dan moeten schoolbesturen aan alle normen voldoen.

Bron: Rijksoverheid.nl

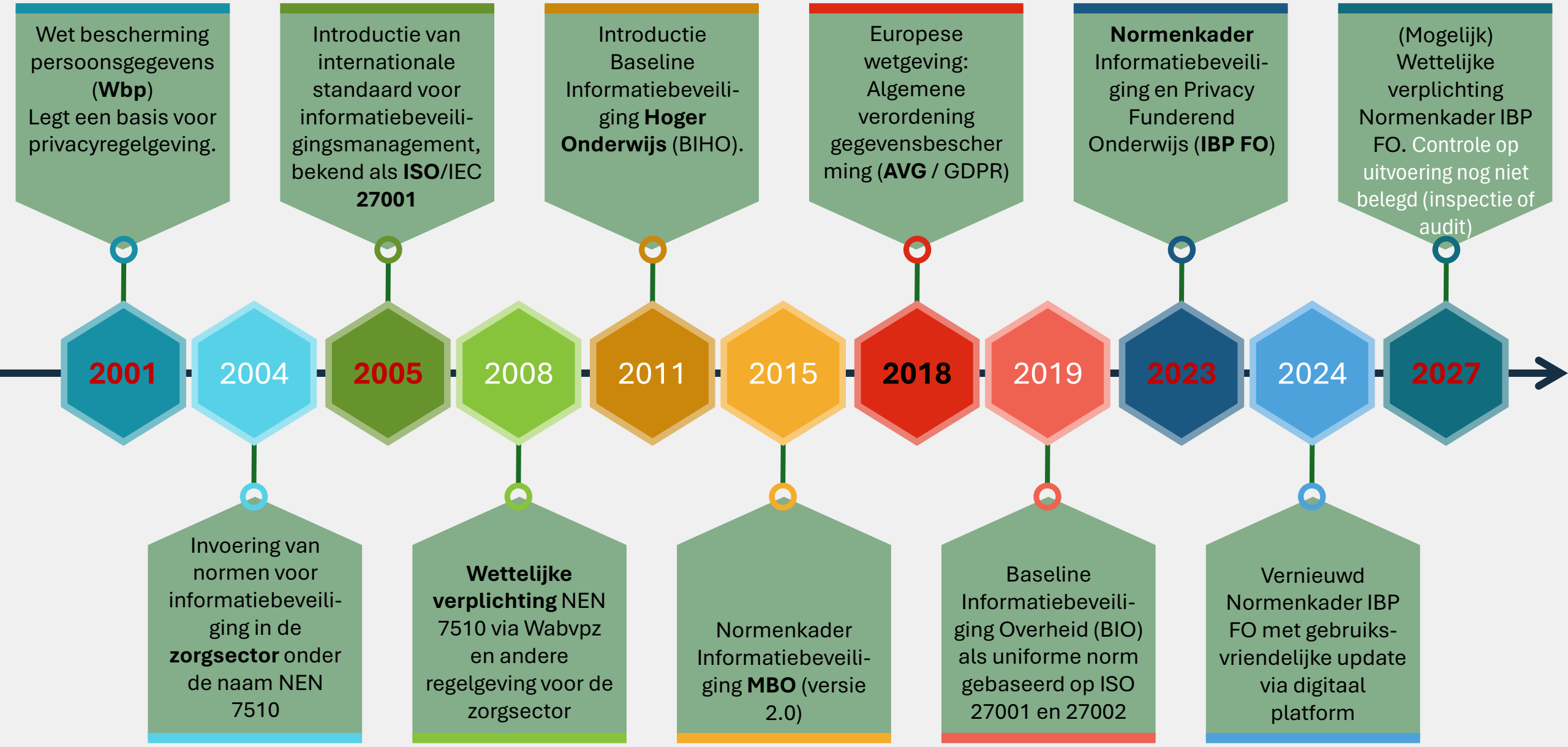


Dit kán toch niet?

- 😠 *“Waarom wij, waarom nu?”*
- 😠 *“Daar komt het ministerie weer.”*
- 😠 *“Daar hebben we ICT toch voor?”*
- 😠 *“We hebben het al zo druk, waar halen we de tijd vandaan?”*
- 😠 *“Kunnen we dit niet uitstellen totdat het écht moet?”*

Een beknopte geschiedenis van het Normenkader IBP FO in vergelijking tot andere sectoren:

ossewold.net
KENNIS • PASSIE • GROEI



Scholen én hun data zijn doelwit

Vier op de vijf scholen dupe van ransomware

01 SEPTEMBER 2023 - 09:52 | ACTUEEL | INNOVATIE & TRANSFORMATIE | SOPHOS

Diederik Toet

Wereldwijd had tachtig procent van de onderwijsinstellingen in 2022 last van ransomware. Dit is beduidend hoger dan een jaar eerder, toen rond de zestig procent van de instellingen zulke aanvallen meldden. De onderwijssector betaalde bovendien relatief vaak het losgeld dat met de datagijzeling is gemoeid. Dit blijkt uit onderzoek van ict-beveiliger Sophos, die oproept om meer te backuppen.

NOS Nieuws • Gisteren, 08:32

Zorgen over online delen kinderfoto's: identiteitsfraude ligt op de loer

In Frankrijk is het illegaal, en het Italiaanse parlement debatteerde onlangs over een nieuwe wet die het strafbaar stelt: ouders die foto's plaatsen van hun kinderen op sociale media. Ook in Nederland maken instanties zich zorgen over de gevolgen van het zogenoemde *sharenting*, een samentrekking van de Engelse woorden *sharing* en *parenting*. Dat slaat op het overmatig delen van kinderfoto's.

NOS Nieuws Sport

NOS Nieuws • Zaterdag 13 april, 13:44

Schoolboekenleverancier Iddink gehackt, mogelijk klantengegevens gelekt

Iddink, een organisatie die schoolboeken en digitaal lesmateriaal verkoopt, is getroffen door een aanval met gijzelsoftware. Dat heeft de organisatie zelf bekendgemaakt.

Door de aanval is mogelijk een groot aantal gegevens gestolen van klanten van Iddink. Het gaat hierbij om persoonlijke informatie zoals namen, e-mailadressen en bankgegevens van leerlingen, ouders en scholen die ooit iets besteld hebben bij Iddink.

Door de aanval heeft Iddink geen toegang meer tot de eigen systemen. Het door klanten gekochte lesmateriaal is wel gewoon beschikbaar, net als het leerlingvolgsysteem Magister, dat onderdeel is van Iddink.

Klanten op de hoogte

Klanten van Iddink zijn op de hoogte gebracht van de aanval. Ook heeft het bedrijf de politie ingeschakeld en de Autoriteit Persoonsgegevens op de hoogte gesteld. Onderzocht wordt hoe groot het datalek is.

Volgens Iddink zit de criminele cybergroep Cactus achter de aanval. Het bedrijf laat weten geen contact te hebben gezocht met Cactus en ook niet bereid te zijn om losgeld te betalen.

Iddink is een van de grootste leveranciers van schoolboeken en digitaal lesmateriaal voor het voortgezet onderwijs in Nederland. Naar eigen zeggen verkoopt en verhuurt

26 vestigingen

Grote hack bij ROC Mondriaan: computers plat en bestanden ontoegankelijk

Door RTL Nieuws
23 augustus 2021 16:29 • Aangepast 23 augustus 2021 16:29

Door onze nieuwsredactie

15 jan 2025 om 18:11
Update: 7 uur geleden

298 reacties | Delen

Hackers die zondag probeerden de computersystemen van de TU Eindhoven aan te vallen, werden volgens vicevoorzitter Patrick Groothuis "op heterdaad betrapt". Sinds de aanval is het netwerk offline en is het onderwijs geschrapt. De universiteit wil de systemen maandag weer online zetten.

Door onze nieuwsredactie

16 jan 2025 om 11:15
Update: 2 uur geleden

142 reacties | Delen

Universiteiten en hogescholen in het zuiden van het land kampen donderdag met een nieuwe ddos-aanval op hun gezamenlijke netwerk. De instellingen hebben last van "trage internetverbindingen of zelfs geen verbinding", meldt ict-coöperatie SURF.

Doel - formeel

- Waarborgen van de **beschikbaarheid**, **integriteit** en **vertrouwelijkheid** van informatie.
- Voldoen aan **relevante wet- en regelgeving**, zoals de AVG.
- Verhogen van het **bewustzijn** rondom informatiebeveiliging binnen de organisatie.

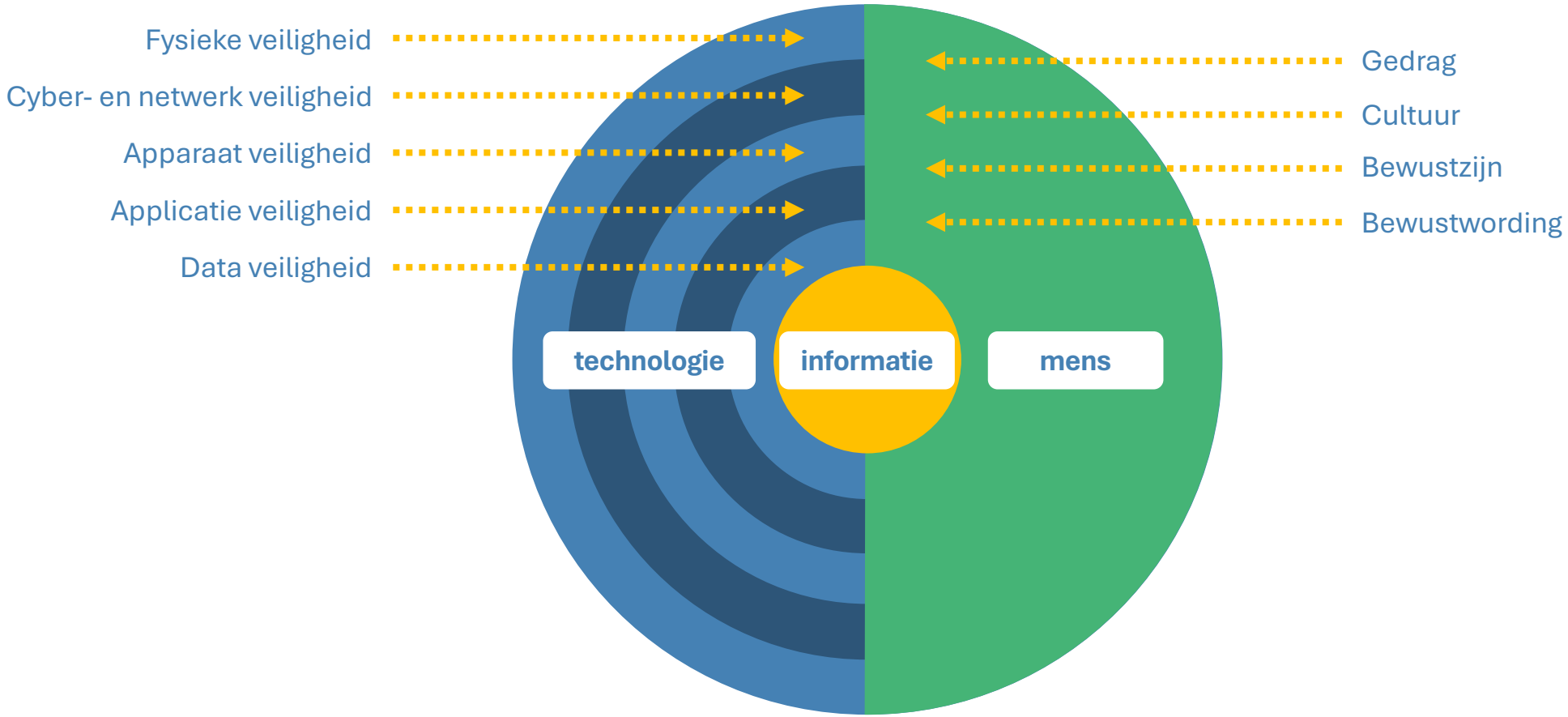
Doel – de kinderen en hún data

https://youtu.be/F4WZ_k0vUDM?si=GrqDeB4mCruw4iID

Archivering op zolder, echt?!

- Let iemand op bewaartermijnen?
- Waar blijft het recht om vergeten te worden?
- Welke gegevens mogen eigenlijk helemaal niet (meer) bewaard worden?
- Wie heeft toegang tot deze data?

Aandachtsgebieden informatiebeveiliging en privacy



Focusgebieden
Eerste jaar = Basis op orde

- IBP-beleid en organisatie *(FG en programmaleider)*
- Veiligheidsbewustzijn *(HR)*
- Incident-, problem-, change management *(ICT)*
- Data- en informatiemanagement *(ICT)*
- Fysieke veiligheid *(Bedrijfsvoering)*
- Bedrijfscontinuïteit en risicomanagement *(Financiën)*
- Basis op orde Privacyregels *(Privacy Officer en FG)*

Thema's van dit jaar:

- Veiligheidsbewustzijn
- Eigenaarschap, rollen, rechten en toegang van (kritische) applicaties
- Risicomanagement, bedrijfscontinuïteit
- Incident-, Problem en Change Management
- Crisismanagement met crisisteam
- Back-Up en herstel
- Governance
- Fysieke toegang, digitale toegang
- Regels voor mobiele apparaten, werken op afstand, datadragers, cameratoezicht, 'gratis' software
- Leveranciersmanagement
- IT Operatie

“Wij beloven

aan onze ouders, leerlingen en medewerkers om als school een veilige en betrouwbare digitale leeromgeving te creëren.”

10 beloften aan ouders en onszelf:

1. We zorgen continu voor een bewust en veilig gebruik van onze digitale middelen door regelmatige trainingen voor alle medewerkers en leerlingen.

2. We reageren snel en effectief op alle cybersecurity incidenten met een professioneel getraind crisisteam.

3. We waarborgen een veilige toegang tot onze systemen en beschermen persoonlijke en schoolgegevens tegen onbevoegden.

4. We garanderen dat aanpassingen aan onze systemen zorgvuldig en veilig worden uitgevoerd, met respect voor privacy en beveiliging.

5. We houden onze digitale omgeving actueel en veilig door regelmatige updates en strikte onderhoudsprocedures.

6. We documenteren en controleren alle digitale processen om de integriteit van onze informatie te waarborgen.

7. We bevorderen openheid en transparantie over hoe we informatie beheren en beschermen, zodat iedereen begrijpt hoe zijn of haar data wordt gebruikt.

8. We zorgen ervoor dat onze digitale leeromgeving voldoet aan alle wettelijke eisen en aan ons schoolbeleid, met regelmatige beoordelingen om deze standaarden te handhaven.

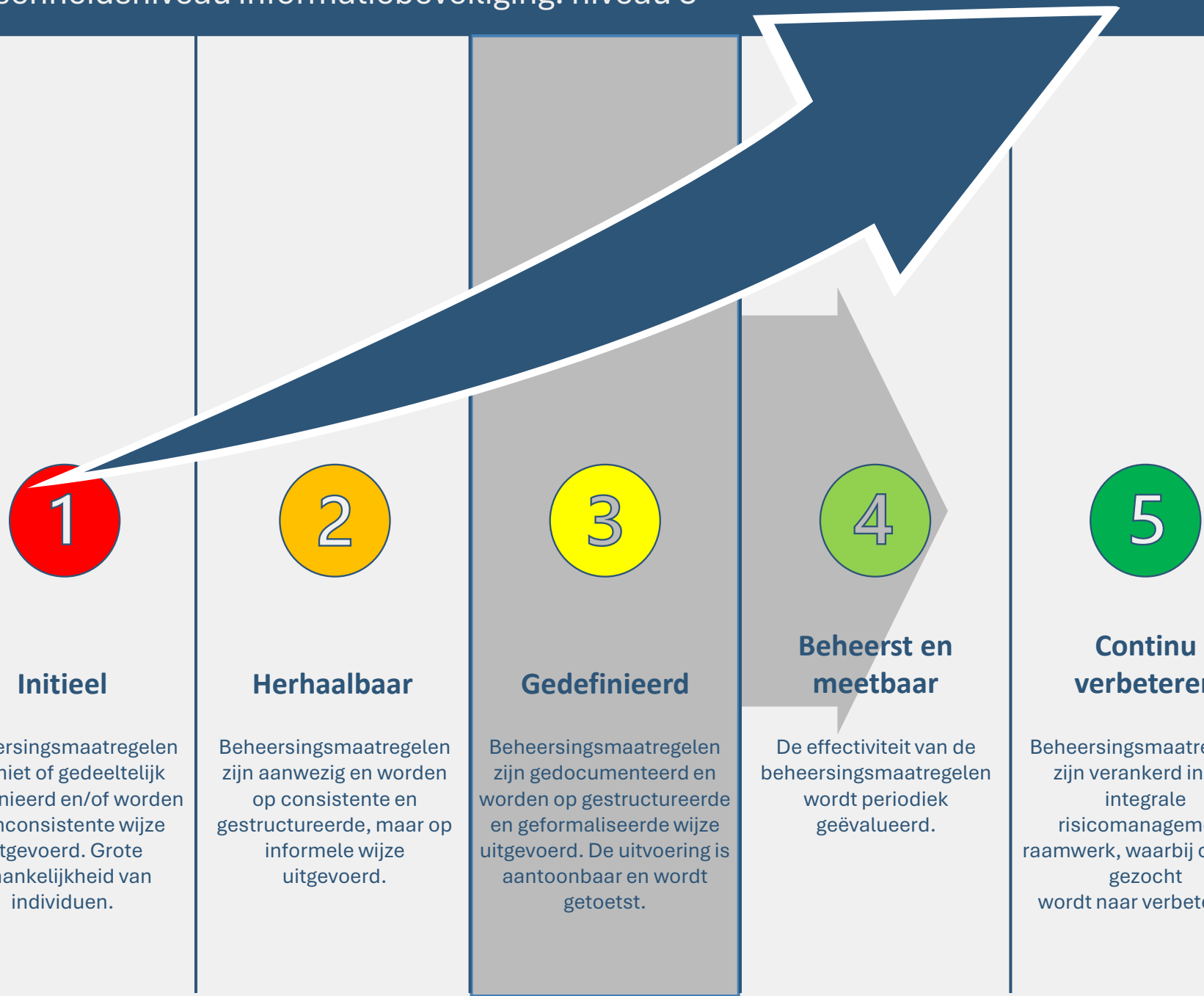
9. We onderhouden sterke relaties met onze leveranciers om te verzekeren dat ook voor hun diensten en producten onze veiligheidsnormen gelden.

10. We zijn toegewijd aan het continu verbeteren van onze procedures om een veilige ondersteunende en educatieve omgeving voor iedereen te garanderen.

Gewenst volwassenheidsniveau informatiebeveiliging: niveau 3+

ossewold.net
KENNIS • PASSIE • GROEI

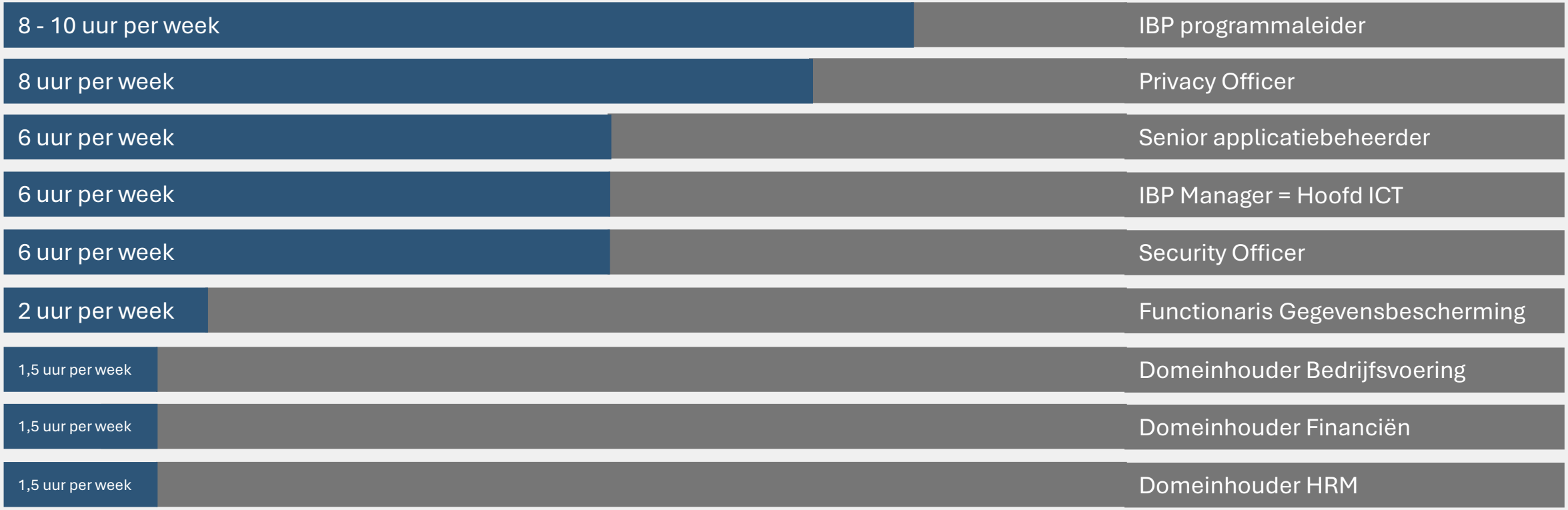
Bron: https://www.NBA.nl gebruikt als norm bij het programma Digitaal Veilig Onderwijs (DVO)



IBP-beleid en organisatie (Domein 1 & 2)

- *IBP-beleidsplan vaststellen*
- *Rollen en verantwoordelijkheden formaliseren*

Tijdsinvestering: projectleiders



Bovenstaand zijn inschattingen, gemaakt door de projectleiders.

Tijdsinvestering: projectbetrokkenen

Bovenstaand zijn voorlopige inschattingen, gemaakt door de programmamanager.

Het Normenkader

Een marathon, géén sprint!

ossewold.net

KENNIS • PASSIE • GROEI

Meer weten?

Paul Ossewold

Digitaal adviseur en programmamanager

paul@ossewold.net

+31 6 158 358 76

www.ossewold.net