

Strategie en visie op informatiebeveiliging en privacy

Versie: 1.3

Uitgaande van de versie van kennisnet van Januari 2025 (aanvulling AR op feb en dec 2025)



Documentgeschiedenis

Revisies

Versie	Datum	Auteur	Review
1		Alex Raaijmakers a.raaijmakers@privaty.nl 06-46757234	Concept 20241205 Voorgaande versie is herzien n.a.v. de vereiste aantoonbare taakgerichte PDCA-aanpak.
2	26-11-2024	Mark van den Bos	Revisie
3	03-01-2025	Maarten Munning	Revisie
4	20-3 & 8-5	Mark van den Bos	Revisie a.d.h.v. input KBG & FG
5	20-11-2025	Richard Mutters	Redigeren van in KBG en CvB behandelde versie tot een beter leesbaar document

Vaststelling

Naam	Functie	Versie	Datum
Ingrid v Doesburg	Voorzitter	0.1 (afgekeurd)	
Ingrid v Doesburg	Voorzitter	1.3 (vastgesteld)	10-02-2026

Documentclassificatie

Classificatie	Beschrijving
Openbaar	Dit document mag zonder beperkingen worden gedeeld
Vertrouwelijk	Dit document mag worden gedeeld met medewerkers van PCBO.
Geheim	Dit document is exclusief bestemd voor medewerkers en samenwerkingspartners van PCBO Rotterdam.

Inhoudsopgave

Inleiding	4
Doelstelling en ambitieniveau	4
Strategie gebaseerd op zeven pijlers	5
Kort samengevat	6

Inleiding

De afhankelijkheid van informatie en ICT in het onderwijs neemt toe, evenals de verwerking van gevoelige gegevens. PCBO Rotterdam staat voor een veilige en verantwoorde omgang met deze informatie.

Deze visie is het fundament van ons IBP-beleid en de implementatie van het nieuwe Normenkader Funderend Onderwijs (IBP-FO), waaraan wij aantoonbaar moeten voldoen (Norm GO.01).

Doelstelling en ambitieniveau

Informatiebeveiliging en Privacy (IBP) staan bij PCBO Rotterdam niet op zichzelf; het is een integraal onderdeel van onze algehele visie op veiligheid en wordt uitgevoerd vanuit vakmanschap, verbondenheid en vertrouwen.

Onze IBP-Inspanningen zijn in de kern gericht op:

- Continuïteit: Waarborgen dat het onderwijs altijd door kan gaan (ICT-middelen zijn bedrijfskritisch).
- Bescherming van Gegevens: Veilig omgaan met persoonsgegevens van leerlingen, collega's en betrokkenen, conform de AVG.
- Transparantie: Duidelijk communiceren over het delen van gegevens met samenwerkende organisaties.
- Bewustzijn: Creëren van bewustzijn over het belang en de waarde van gegevensveiligheid bij alle betrokkenen.

Relatie tussen IBP en Privacy

- Informatiebeveiliging: Richt zich op het beheersen van risico's door de Beschikbaarheid (continuïteit), Integriteit (betrouwbaarheid) en Vertrouwelijkheid (exclusiviteit) van alle informatie te waarborgen.
- Privacy (AVG): Draait om de zorgvuldige omgang met persoonsgegevens ter bescherming van de grondrechten van betrokkenen.

Conclusie: Informatiebeveiliging is een noodzakelijke voorwaarde om te voldoen aan de eisen van de AVG.

Ambitie

Wij volgen wet- en regelgeving nauwgezet. PCBO streeft ernaar om in 2027 te voldoen aan volwassenheidsniveau 3 van het Normenkader IBP-FO.

Strategie gebaseerd op zeven pijlers

Onze strategie bestaat uit zeven kernprincipes die leidend zijn voor alle IBP-activiteiten:

1. Eindverantwoordelijkheid bij het Bestuur

- Het Schoolbestuur is eindverantwoordelijk en legt hierover verantwoording af.
- De Schoolleiding heeft een gedelegeerde verantwoordelijkheid voor de uitvoering van het IBP-beleid binnen de eigen school.

2. Risicogebaseerd Werken

- Alle maatregelen zijn gericht op het beheersen van actuele risico's en dreigingen.
- Informatie en ICT-systemen worden geclassificeerd op basis van BIV-eisen (Beschikbaarheid, Integriteit, Vertrouwelijkheid).
- De classificatie bepaalt de te treffen maatregelen, waarbij er een balans is tussen af te dekken risico's en benodigde investeringen.
-

3. Informatiebeveiliging is een Continu Proces

- IBP is nooit 'af'. We evalueren maatregelen ten minste jaarlijks.
- Leren van Incidenten: Incidenten zien we als een leermoment om onze beveiliging verder te versterken.
- Proactieve Bescherming: We investeren in preventie en veerkracht tegen cyberdreigingen (hacking, datalekken, ransomware).

4. Iedereen Heeft een Rol

- Veilig en betrouwbaar omgaan met informatie (digitaal én papier) is de verantwoordelijkheid van iedereen binnen PCBO Rotterdam.
- Leidinggevenden maken de dagelijkse risicoafwegingen en zorgen voor passende beveiligingsmaatregelen.

5. Investering in Mensen, Processen én Technologie

- Effectieve IBP wordt bereikt door de doeltreffende inzet van deze drie factoren; het kan niet alleen met techniek worden opgelost.
- Technologie ontlast: Waar mogelijk kiezen we voor technologische oplossingen om de medewerkers en leerlingen te ontlasten van continue beoordelingsvermogen.

6. Security en Privacy by Design

- Bij elke wijziging, aanschaf van nieuwe ICT-middelen of uitbesteding van clouddiensten, wordt vooraf gekeken naar de IBP-impact.
- Dit gebeurt door middel van een Pre-DPIA (Data Protection Impact Assessment) en een beoordeling van de Verwerkersovereenkomst.
- Toegang: Medewerkers en leerlingen krijgen alleen toegang tot de systemen en informatie die zij vanuit hun rol nodig hebben.

7. We Doen Het Samen (De Keten)

- We geloven in een open cultuur en het delen van inzichten om problemen snel op te lossen. De schuldvraag staat nooit een oplossing in de weg.
- We werken met een GRC-systematiek (Governance, Risk & Compliance) om processen te structureren en naleving te borgen.
- Externe Partners: Wij eisen van leveranciers van onderwijsleermiddelen en ICT-partners dat zij aantoonbaar, bewezen en gecertificeerd voldoen aan de IBP-FO-normen om ons proactief te ontzorgen.
- Betrokkenheid: We informeren medewerkers, ouders en leerlingen transparant over welke gegevens we verwerken, hoe ze beveiligd zijn en met wie ze worden gedeeld.

Kort samengevat

Informatiebeveiliging en cybersecurity zijn complex en risicovol. PCBO Rotterdam beantwoordt deze uitdaging door:

1. De IBP-FO-standaard integraal te beantwoorden en te waarborgen op bestuurlijk, beleidsmatig en operationeel niveau.
2. Het risico en de naleving te bewaken in het GRC-systeem (PCC).
3. Externe partners in te schakelen voor beheer en expertise.

Dit waarborgt de continuïteit van het onderwijs, de privacy van leerlingen en medewerkers, en onze morele verplichting tegen cybercriminaliteit.