Strategie en Visie op IBP-beleid
Schoolvereniging Rehoboth

REHOBOTH
Vereniging voor Scholen met de Bijbel

Versie	Status	Datum	Auteur	IBP norm
1.0	concept	13-11-2025	LdB PoS	IB 1; GO.01
1.1	concept	26-01-2026	C. Doornbos	IB 1; GO.01
1.1	vastgesteld	04-03-2026	C. Doornbos	IB 1; GO.01

Opgesteld door Privacy op School, gebaseerd op het template van Kennisnet[1]

1

Inhoudsopgave

[1]Dit template is opgesteld door Kennisnet en verschijnt onder de licentie Creative Commons Naamsvermelding 4.0 Nederland

Inleiding

Schoolvereniging Rehoboth is in toenemende mate afhankelijk van digitale informatie en ICT. Wij verwerken steeds meer en steeds gevoeligere informatie. Daarom vinden we het belangrijk om veilig en verantwoord met die informatie om te gaan en deze goed te beschermen, want de afhankelijkheid van informatie en ICT brengt kwetsbaarheden en risico's met zich mee.

In dit document beschrijft Schoolvereniging Rehoboth haar visie en strategie voor informatiebeveiliging en privacy. Visie en strategie vormen samen de context voor het opstellen van het beleid voor informatiebeveiliging en privacy (IBP-beleid). Onze visie op informatiebeveiliging en privacy is hierbij de stip op de horizon. We beschrijven wat we op het gebied van informatiebeveiliging en privacy willen bereiken en waarom. De strategie voor informatiebeveiliging en privacy vertaalt deze visie in een concrete aanpak. In de strategie beschrijven we hoe we de visie in de praktijk brengen.

1 Visie op informatiebeveiliging en privacy

Informatiebeveiliging en privacy staat bij Schoolvereniging Rehoboth niet op zichzelf. We spannen ons in om informatie te beveiligen en veilig om te gaan met persoonsgegevens, om zo bij te dragen aan het realiseren van onze organisatiedoelen**:**

1.1 Onze missie en visie op onderwijs

Ontwikkeling met lef en liefde!

Onze Missie
Schoolvereniging Rehoboth geeft kinderen zo mogelijk thuis nabij een onderwijsaanbod dat past bij de onderwijsbehoefte van de leerling. Dit gebeurt zo mogelijk geïntegreerd in een reguliere setting. De onderwijsbehoefte van de leerling is daarbij bepalend. Leerlingen blijven zoveel mogelijk op een reguliere basisschool. Iedere basisschool binnen de vereniging biedt de basisondersteuning zoals verwoord door middel van de standaarden basisondersteuning uit het referentiekader. Iedere school dient een onderwijsaanbod te hebben voor kinderen met een minder of meer dan gemiddelde intelligentie, voor kinderen met leerproblemen (bijvoorbeeld als gevolg van dyslexie/ dyscalculie) en voor kinderen met extra onderwijsbehoeften op het gebied van gedrag.

.

Onze Visie: Geloof in onderwijs
Het Woord van God is niet alleen leidend in het onderwijs dat wordt gegeven, maar komt ook tot uiting op de manier waarop leerlingen en mensen met elkaar omgaan. Dat geldt ook voor de manier waarop passend onderwijs wordt vormgegeven.

Onze inspanningen op het gebied van informatiebeveiliging en privacy zijn gericht op:

- Het beschermen van persoonsgegevens van leerlingen, ouders en medewerkers.
- Het waarborgen van de continuïteit van het onderwijs.
- Veilig omgaan met persoonsgegevens volgens de regels van de AVG.

1.2 Hulpmiddelen

De volgende hulpmiddelen zetten we in om onze visie te waarborgen:

- We stellen het **IBP-beleidsplan** vast. Hierin beschrijven we, zoals het Normenkader IBP voorschrijft, ons beleid en de manier waarop we informatiebeveiliging en privacy binnen de organisatie borgen.
- In het **IBP-beleidsplan** wordt niet alleen het beleid uiteengezet, maar ook concreet gemaakt hoe dit beleid in de praktijk wordt uitgevoerd. Er zijn actiepunten per kalenderjaar opgenomen, waardoor het document levend en dynamisch blijft en voortdurend aansluit bij actuele risico's en ontwikkelingen.
- Jaarlijks wordt een **risicoanalyse** uitgevoerd om potentiële bedreigingen en kwetsbaarheden systematisch te identificeren en te beoordelen. Op basis van de resultaten worden gerichte verbetermaatregelen genomen, zodat risico's proactief worden gemanaged in plaats van reactief opgelost.
- **Technische maatregelen** zoals antivirussoftware, firewalls, versleuteling van gevoelige gegevens, een streng wachtwoordbeleid en multi-factor authenticatie (MFA) vormen

een belangrijke verdedigingsraad tegen externe en interne bedreigingen. Deze maatregelen zorgen ervoor dat toegang tot systemen en gegevens zorgvuldig wordt gecontroleerd en dat kritieke informatie beschermd is tegen onbevoegde toegang of verlies.

- Jaarlijks voeren we **bewustwordingsactiviteiten** uit om medewerkers, leerlingen en andere betrokkenen alert te houden op hun rol binnen informatiebeveiliging en privacy. Denk hierbij aan workshops, e-learningmodules, campagnes en korte bewustmakingsacties rondom actuele dreigingen zoals phishing of datalekken.
- Er is een **centraal meldpunt** ingericht voor het melden van beveiligingsincidenten of (mogelijke) datalekken. Dit meldpunt is laagdrempelig bereikbaar via de website en het intranet, waardoor snelle melding en opvolging mogelijk wordt gemaakt. Zo kunnen incidenten snel worden onderzocht en passende maatregelen worden getroffen.
- We **werken samen met externe experts** zoals Privacy op School, YourSafetyNet en PEP Onderwijsadvies. Door deze samenwerkingen blijven we up-to-date met best practices, nieuwe regelgeving en actuele dreigingen en kunnen we terugvallen op specialistische kennis wanneer dat nodig is.

Door deze combinatie van structureel beleid, technische beveiligingsmaatregelen, bewustwording, een meldstructuur en externe expertise, creëren we een robuust fundament voor informatiebeveiliging en privacy. Zo zorgen we ervoor dat onze visie niet alleen op papier staat, maar ook daadwerkelijk wordt nageleefd en continu verbeterd. Onvoldoende informatiebeveiliging kan leiden tot ongewenste risico's in het onderwijsproces en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële en/of imago-schade.

1.3 Relatie met privacy

De bescherming van persoonsgegevens (privacy) is gerelateerd aan informatiebeveiliging, maar is niet hetzelfde. Informatiebeveiliging gaat over het verminderen van beveiligingsrisico's door het waarborgen van vertrouwelijkheid, integriteit en beschikbaarheid van informatie. Dat doet Rehoboth in lijn met de prioriteiten en doelen van haar organisatie. De bescherming van persoonsgegevens heeft betrekking op de verantwoorde omgang met persoonsgegevens om zo de (grond)rechten van degenen op wie ze betrekking hebben te waarborgen.
De Algemene Verordening Gegevensbescherming (AVG) stelt eisen aan de omgang van persoonsgegevens. Een van die eisen is dat je persoonsgegevens beveiligt. Daarmee is informatiebeveiliging een onderwerp op zich én onderdeel van de bescherming van persoonsgegevens.

1.4 Wet- en regelgeving en het Normenkader IBP

Om persoonsgegevens te beschermen en de continuïteit van het onderwijs te waarborgen, zijn op het risico afgestemde maatregelen nodig. Daarom kiezen we ervoor om ontwikkelingen op het gebied van wet- en regelgeving nauwlettend te volgen en daaraan zo snel mogelijk te voldoen. Dit is terug te zien in onze compliance aan het voldoen aan de AVG en onze inspanningen om aan het Normenkader IBP te voldoen. Ons streven is om per augustus 2027 minimaal op volwassenheidsniveau 2,5 te scoren, waarbij we voor wat betreft de normen van het P(rivacy)-deel het volwassenheidsniveau 3 willen behalen, zodat we aantoonbaar compliant zijn aan de AVG.

2 Strategie voor informatiebeveiliging en privacy

De strategie voor informatiebeveiliging en privacy van Schoolvereniging Rehoboth bestaat uit zeven pijlers, die steeds terugkomen in de activiteiten die we ondernemen om IBP te versterken.

2.1 Het bestuur is eindverantwoordelijk

Het bestuur van Schoolvereniging Rehoboth neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging geregeld wordt. Het bestuur is hierop aan te spreken en het legt hier verantwoording over af. Zo rapporteren wij in de continuïteitsparagraaf van onze jaarrapportage[2] over de aanwezigheid en werking van het interne risicobeheersings- en controlesysteem en worden de belangrijkste risico's en onzekerheden beschreven. Ook rapporteren wij over privacy gerelateerde onderwerpen zoals welke datalekken er zijn verholpen en hebben geleid tot herziening van bestaand beleid of ervoor hebben gezorgd dat we nieuw beleid hebben geïntroduceerd.
De schoolleiding van onze locaties heeft een gedelegeerde verantwoordelijkheid voor de toepassing van het IBP-beleid binnen de eigen school. Het bestuur en de schoolleiding spreken regelmatig over de effectiviteit van het beleid in de praktijk.

2.2 We werken risico gebaseerd

Informatiebeveiliging en de toepassing van de AVG zijn bedoeld om risico's te beheersen. Alle getroffen maatregelen dragen daaraan bij. De beheersing van risico's maakt integraal onderdeel uit van de algemene risicobeheersing binnen Rehoboth. Prioriteiten binnen de informatiebeveiliging en privacy worden gesteld op basis van de actuele stand van dreigingen en risico's.
Rehoboth classificeert informatie en ICT-systemen. De classificatie is het uitgangspunt voor maatregelen die we treffen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen voor de te treffen maatregelen.

2.3 Informatiebeveiliging is een continu proces

Informatiebeveiliging is bij Schoolvereniging Rehoboth een continu proces. Regelmatig, en ten minste jaarlijks, evalueren we getroffen maatregelen en overwegen we of aanpassing gewenst is.
Onze informatiebeveiliging is nooit 'af'. Als er incidenten plaatsvinden, zien we dat als een gelegenheid om te leren, zodat we onze informatiebeveiliging verder kunnen versterken. We gaan op zoek naar de onderliggende oorzaken en werken samen om deze op te lossen.

---

[2] *Handreiking bestuursverslag po 2024* Pag 18, Continuiteitsparagraaf:
Informatiebeveiliging en privacy (IBP) (B3) Over dit thema, aangewezen door de Minister van OCW, moeten schoolbesturen zich op grond van de Regeling jaarverslag artikel 4 lid 6 nader verantwoorden.

2.4 Iedereen heeft een rol in informatiebeveiliging en privacy

Binnen Schoolvereniging Rehoboth is het veilig en betrouwbaar omgaan met informatie en persoonsgegevens de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie en persoonsgegevens, maar ook van papieren documenten.
Schoolleiders en andere leidinggevenden hebben in de dagelijkse uitvoering van het IBP-beleid een sleutelrol. Zij maken risicoafwegingen en zakelijke keuzes, waarop de technische maatregelen worden afgestemd. Het schoolbestuur zorgt dat zij kunnen beschikken over de expertise die hiervoor nodig is.

2.5 We investeren in mensen, processen én technologie

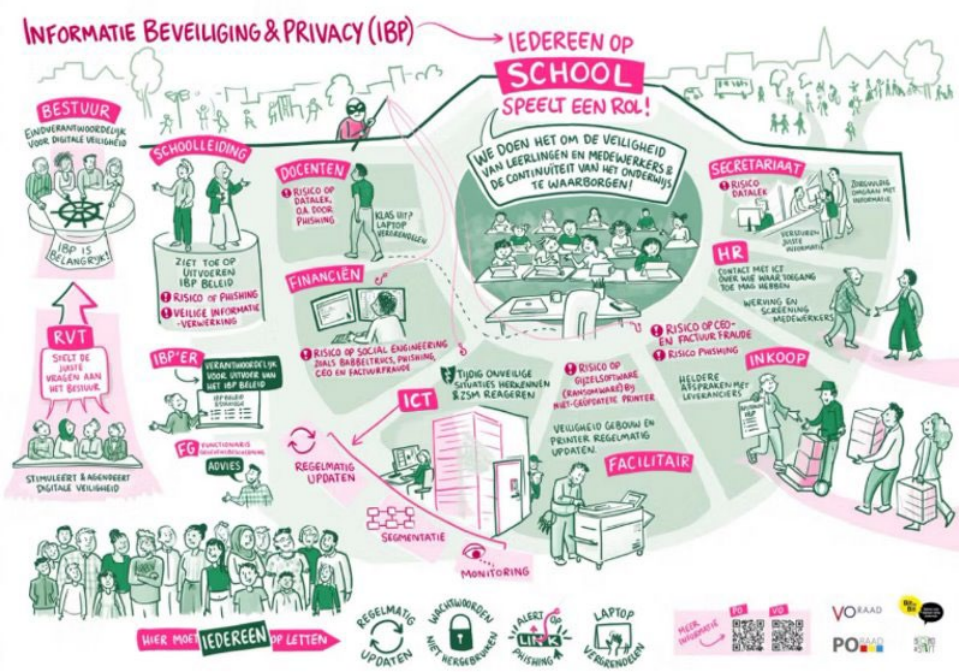
Effectieve informatiebeveiliging en privacy bestaat uit de doeltreffende inzet van mensen, processen en technologie. Al deze drie factoren zijn nodig: IBP kan niet alleen met techniek opgelost worden. Ook hoort het onderwerp niet alleen thuis bij de ICT-afdeling.
Hoewel IBP uit meer bestaat dan alleen technologie, zijn technologische oplossingen wel degelijk onmisbaar. Ze dragen bij aan het creëren van een veilige digitale leer- en werkomgeving. Tegelijk werken we ook aan bewustwording en gedrag dat passend is in een veilige (digitale) omgeving. Ook de leerlingen rusten we daar in toe.

2.6 We kiezen voor security en privacy by design

Schoolvereniging Rehoboth kijkt bij wijzigingen in de infrastructuur of de aanschaf van nieuwe ICT-systemen vooraf naar de impact hiervan op informatiebeveiliging en gevolgen voor privacy. Zo kunnen tijdig de juiste maatregelen getroffen worden. Dit geldt ook wanneer we clouddiensten gebruiken of ICT-functionaliteit uitbesteden. Ook dan brengen we IBP tijdig ter sprake, zodat we vooraf en tijdens het gebruik steeds zekerheid hebben over de getroffen maatregelen.
Medewerkers en leerlingen hebben alleen toegang tot informatie en ICT-systemen die ze vanuit hun rol of werkzaamheden nodig hebben.

2.7 We doen het samen

Bij Schoolvereniging Rehoboth streven we naar een open cultuur, waarin we informatie en inzichten voortvarend delen. Zo kunnen we problemen snel ontdekken en oplossen. Samen zoeken we naar effectieve en passende oplossingen voor uitdagingen.
Bij onze inspanningen staan we niet alleen. We trekken samen op met andere schoolbesturen, om van elkaar te leren en de lasten te verdelen. Daarvoor sluiten we aan bij regionale en landelijke initiatieven.


INFORMATIE BEVEILIGING & PRIVACY (IBP)
IEDEREEN OP
SCHOOL
SPEELT EEN ROL!
WE DOEN HET OM DE VEILIGHEID VAN LEERLINGEN EN MEDEWERKERS & DE CONTINUÏTEIT VAN HET ONDERWIJS TE WAARBORGEN!
BESTUUR
EINDVERANTWOORDELIJK VOOR DIGITALE VEILIGHEID
IBP IS BELANGRIJK!
RVT
STELT DE JUISTE VRAGEN AAN HET BESTUUR
STIMULEERT & AGENDEERT DIGITALE VEILIGHEID
SCHOOLLEIDING
ZIET TOE OP UITVOEREN IBP BELEID
RISICO OP PHISHING
VEILIGE INFORMATIE-VERWERKING
DOCENTEN
RISICO OP DATALEK, DA DOOR PHISHING
KLAS UIT? LAPTOP VERGRENDELEN
FINANCIËN
RISICO OP SOCIAL ENGINEERING ZOALS BABBELTRUCS, PHISHING, CEO EN FACTUURFRAUDE
IBP'ER
VERANTWOORDELIJK VOOR UITVOER VAN HET IBP BELEID
FG FUNCTIONARIS GEGEVENSBESCHERMING
ADVIES
ICT
REGELMATIG UPDATEN
SEGMENTATIE
MONITORING
TIJDIG ONVEILIGE SITUATIES HERKENNEN & ZSM REAGEREN
RISICO OP GIJZELSOFTWARE (RANSOMWARE) BIJ NIET-GEÜPDATETE PRINTER
VEILIGHEID GEBOUW EN PRINTER REGELMATIG UPDATEN
FACILITAIR
SECRETARIAAT
RISICO DATALEK
VERSTUREN JUISTE INFORMATIE
ZORGVULDIG OMGAAN MET INFORMATIE
HR
CONTACT MET ICT OVER WIE WAAR TOEGANG TOE MAG HEBBEN
WERVING EN SCREENING MEDEWERKERS
RISICO OP CEO- EN FACTUUR FRAUDE
RISICO PHISHING
INKOOP
HELDERE AFSPRAKEN MET LEVERANCIERS
HIER MOET IEDEREEN OP LETTEN
REGELMATIG UPDATEN
WACHTWOORDEN NIET HERGEBRUIKEN
ALERT OP LINKS PHISHING
LAPTOP VERGRENDELEN
MEER INFORMATIE
VO
VO RAAD
PO RAAD