

Strategie en visie op informatiebeveiliging en privacy

Voorbeelddocument

Versie: Januari 2025



**Let op: verwijder deze pagina voor gebruik**

**Over dit voorbeelddocument**

**Dit voorbeelddocument helpt je met het maken van een eigen** **visie en strategie op informatiebeveiliging en privacy (IBP). Elke school en elk schoolbestuur is anders. Pas het proces daarom aan aan jouw eigen situatie.**

**Aanpassen van dit voorbeelddocument**

Let bij het aanpassen van het document op het volgende:

* Bij hoofdstukken en paragrafen zijn soms toelichtingen geplaatst. Verwijder deze voordat je het document definitief maakt.
* Geel gearceerde teksten moet je vervangen door eigen tekst.

**Totstandkoming**

Dit voorbeelddocument is samengesteld door Kennisnet. Binnen het programma Digitaal Veilig Onderwijs bundelen het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en de VO-raad hun krachten voor een onderwijssector waarin iedere leerling digitaal veilig kan leren en medewerkers digitaal veilig kunnen werken.

**Sommige rechten voorbehouden**

Hoewel aan dit document de uiterste zorg is besteed, aanvaardt Kennisnet geen aansprakelijkheid voor eventuele fouten of onvolkomenheden. Ook aanvaardt Kennisnet geen enkele aansprakelijkheid voor schade van welke aard dan ook, ontstaan uit het (onjuiste) gebruik van dit document.



Dit template is opgesteld door Kennisnet en verschijnt onder de licentie [*Creative Commons Naamsvermelding 4.0 Nederland*](https://creativecommons.org/licenses/by/4.0/legalcode.nl).

**Vragen?**

Heb je vragen over dit voorbeelddocument? Kijk voor meer informatie op [*normenkaderibp.kennisnet.nl/groeipad*](file:///Users/jhgerrits/Documents/1.%20Kennisnet%20voorbeeldocumenten/normenkaderibp.kennisnet.nl/groeipad)of stuur een mail naar *ibp@kennisnet.nl**.*

**Documentgeschiedenis**

***Toelichting***

* *Vul in wie dit document vaststelt.*
* *Geef aan of het document openbaar, vertrouwelijk of geheim is en wie het in die gevallen mogen zien.*

**Revisies**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Auteur** | **Review** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Vaststelling**

|  |  |  |  |
| --- | --- | --- | --- |
| **Naam** | **Functie** | **Versie** | **Datum** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Documentclassificatie**

|  |  |
| --- | --- |
| **Classificatie** | **Beschrijving** |
| Openbaar | Dit document mag zonder beperkingen worden gedeeld |
| Vertrouwelijk | Dit document mag worden gedeeld met medewerkers van <naam schoolbestuur en eventuele andere organisaties>. |
| Geheim | Dit document is exclusief bestemd voor de volgende personen: <bijv. leden MT>. |

**Inhoudsopgave**

[Inleiding 5](#_Toc189080720)

[Visie op informatiebeveiliging en privacy 6](#_Toc189080721)

[Relatie met privacy 6](#_Toc189080722)

[Ambitieniveau 6](#_Toc189080723)

[Strategie voor informatiebeveiliging en privacy 8](#_Toc189080724)

[1. Het schoolbestuur is eindverantwoordelijk 8](#_Toc189080725)

[2. We werken risicogebaseerd 8](#_Toc189080726)

[3. Informatiebeveiliging is een continu proces 8](#_Toc189080727)

[4. Iedereen heeft een rol in informatiebeveiliging en privacy 8](#_Toc189080728)

[5. We investeren in mensen, processen én technologie 9](#_Toc189080729)

[6. We kiezen voor security en privacy by design 9](#_Toc189080730)

[7. We doen het samen 9](#_Toc189080731)

# Inleiding

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. Scholen verwerken steeds meer en steeds gevoeligere informatie. Bij <naam schoolbestuur> 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.

Dit document beschrijft de visie en strategie voor informatiebeveiliging en privacy van <naam schoolbestuur>. De visie en strategie vormen samen de context voor het opstellen van het beleid voor informatiebeveiliging en privacy (IBP-beleid). De visie op informatiebeveiliging en privacy is hierbij de stip op de horizon. Deze beschrijft 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.

# Visie op informatiebeveiliging en privacy

***Toelichting***

* *Je visie op informatiebeveiliging en privacy volgt uit de missie of doelen die je als organisatie hebt. Vul in de paragraaf hieronder die missie of organisatiedoelen in:*

Informatiebeveiliging en privacy staat bij <naam schoolbestuur> 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**:**

<Vul de organisatiedoelen of missie van het schoolbestuur in>

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

* Het beschermen van persoonsgegevens.
* Het waarborgen van de continuïteit van het onderwijs.
* Veilig omgaan met persoonsgegevens volgens de regels van de AVG.

## 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 doe je in lijn met de prioriteiten en doelen van de 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. Zo is informatiebeveiliging dus een onderwerp op zichzelf en is het daarnaast onderdeel van de bescherming van persoonsgegevens.

## Ambitieniveau

***Toelichting***

* *Je moet voor deze paragraaf te kiezen uit twee opties. Haal degene die niet van toepassing is weg. Bij optie 1 “Wet- en regelgeving leidend” en zorg je dat je daaraan voldoet. Bij optie 2 ga je nog een stap verder. De eisen die volgen uit wet- en regelgeving zijn dan het minimum. Je kijkt steeds of je nog meer kan doen dan dat.*

<Optie 1: Wet- en regelgeving is leidend>

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 mogelijke te voldoen.

<Optie 2: Wet- en regelgeving is minimumniveau>

Om persoonsgegevens te beschermen en de continuïteit van het onderwijs te waarborgen, zijn op het risico afgestemde maatregelen nodig. We zien de ontwikkelende wet- en regelgeving als een minimumniveau van beveiliging. We zullen steeds overwegen of het niveau van de ontwikkelende wet- en regelgeving voor ons hoog genoeg is en anders aanvullende maatregelen treffen om te zorgen dat informatie binnen de ICT-systemen van <naam schoolbestuur> steeds uitstekend beschermd is.

# Strategie voor informatiebeveiliging en privacy

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

## 1. Het schoolbestuur is eindverantwoordelijk

Het schoolbestuur van <naam schoolbestuur> 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.

De schoolleiding van individuele scholen heeft een gedelegeerde verantwoordelijkheid voor de toepassing van het IBP-beleid van het schoolbestuur binnen de eigen school. Het schoolbestuur en de schoolleiding spreken regelmatig over de effectiviteit van het beleid in de praktijk.

## 2. We werken risicogebaseerd

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 <naam schoolbestuur>. Prioriteiten binnen de informatiebeveiliging en privacy worden gesteld op basis van de actuele stand van dreigingen en risico's.

<Naam schoolbestuur> 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.

## 3. Informatiebeveiliging is een continu proces

Informatiebeveiliging is bij <naam schoolbestuur> 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.

## 4. Iedereen heeft een rol in informatiebeveiliging en privacy

Binnen <naam schoolbestuur> 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.

## 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. Door waar mogelijk voor technologische oplossingen te kiezen, ontlasten we de aandacht en het beoordelingsvermogen van onze leerlingen en medewerkers.

## 6. We kiezen voor security en privacy by design

<Naam schoolbestuur> 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.

## 7. We doen het samen

Bij <naam schoolbestuur> streven we naar een open cultuur, waarin we informatie en inzichten voortvarend delen. Zo kunnen we problemen snel ontdekken en oplossen. De schuldvraag mag nooit in de weg staan aan een effectieve en passende oplossing.

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.