

Plan bewustwordingsprogramma

Voorbeelddocument

Versie: Februari 2025



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

**Over dit voorbeelddocument**

**Dit voorbeelddocument helpt je met het maken van een plan voor een bewustwordingsprogramma. 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 de procesbeschrijving definitief maakt.
* Deze procesbeschrijving gaat ervan uit dat taken, rollen en functies die nodig zijn om het proces uit te voeren bij de juiste personen belegd zijn. Is dit niet zo? Ga dan eerst naar fase 1 van het Groeipad.
* 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***

* *Geef hier aan wie het document vaststelt. Dat kan bijvoorbeeld de proceseigenaar zijn, maar ook het bestuur.*
* *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**

[1 Inleiding 5](#_Toc191393476)

[1.1 Aansturing, budget en borging 5](#_Toc191393477)

[1.2 Nulmeting en risico’s rond digitaal veilig werken 6](#_Toc191393478)

[2 Het bewustwordingsprogramma 7](#_Toc191393479)

[2.1 Scope en strategie 7](#_Toc191393480)

[2.2 Doelgroep 7](#_Toc191393481)

[2.3 Doelstelling 7](#_Toc191393482)

[2.4 Bewustwordingsmiddelen en planning 8](#_Toc191393483)

[3 Effect meten, evalueren en verbeteren 10](#_Toc191393484)

# Inleiding

Beleid en technische maatregelen zijn niet voldoende om risico’s op het terrein van informatiebeveiliging en privacy (IBP) uit te sluiten. De mens is hierin ook een belangrijke factor. Aandacht verslapt snel. Daarom is het nodig om het bewustzijn van medewerkers over de verantwoordelijkheden die ze hebben voortdurend aan te scherpen. Op die manier verhogen we de kennis van bestaande risico’s en moedigen we veilig en verantwoord gedrag aan. Hiervoor neemt <naam schoolbestuur> de volgende maatregelen:

* Er is een bewustwordingsprogramma dat <invullen herzieningstermijn> wordt herzien waarin de bewustwordingsactiviteiten en de verantwoordelijkheden voor deze activiteiten worden beschreven.

Het bewustwordingsprogramma sluit aan bij de strategie en visie van <naam schoolbestuur> op IBP. De concrete invulling van de strategie en visie staan beschreven in het IBP-beleid. Met dit bewustwordingsprogramma verankert <naam schoolbestuur> digitaal veilig werken in de organisatie

##  Aansturing, budget en borging

***Toelichting***

* *Omschrijf de wijze waarop het programma wordt aangestuurd en ingebed in de organisatie en wie waarvoor verantwoordelijk is.*
* *Neem het budget op in het plan.*

Het schoolbestuur ziet bewustwording op het gebied van IBP als een strategische prioriteit en investeert hierin door voldoende budget en capaciteit vrij te maken. Het schoolbestuur en schoolleiders dragen actief bij aan digitaal veilig werken door het belang van IBP zichtbaar uit te dragen in houding en gedrag.

Het uitgangspunt is dat de continuïteit van het onderwijs wordt gewaarborgd, de persoonlijke levenssfeer van de betrokkenen wordt gerespecteerd en <naam schoolbestuur> voldoet aan relevante wet- en regelgeving. Dit gebeurt onder andere door bewustwording te vergroten van het belang van het zorgvuldig omgaan met informatie, systemen en persoonsgegevens.

Verantwoordelijkheden:

* <Naam schoolbestuur> is verantwoordelijk voor het formeel goedkeuren van het bewustwordingsprogramma.
* <Functietitel> is verantwoordelijk voor het opstellen en het beheren van het bewustwordingsprogramma.

Het schoolbestuur heeft een budget vrijgemaakt voor het realiseren van een bewustwordingsprogramma. Dit budget wordt jaarlijks vastgesteld in het jaarplan. Daarnaast maakt het schoolbestuur uren en middelen vrij voor het opstellen en beheren van het programma door <functietitel>. Ook faciliteert het bestuur dat medewerkers kunnen deelnemen aan het programma.

## Nulmeting en risico’s rond digitaal veilig werken

***Toelichting***

* *Om te bepalen wat de grootste aandachtspunten in je organisatie zijn op het gebied van digitaal veilig gedrag, breng je de belangrijkste risico's in kaart waarin gedrag het verschil kan maken.*
* *Digitaal onveilig gedrag kan verschillende oorzaken hebben: een gebrek aan kennis of motivatie, te hoge werkdruk of een technisch probleem. Zorg dat helder is wat de oorzaak van onveilig gedrag is.*
* *Om het effect van het bewustwordingsprogramma te meten, doe je vooraf een nulmeting om het niveau van de medewerkers te bepalen. Dit kun je bijvoorbeeld doen met enquêtes en interviews.*

<Naam schoolbestuur> heeft een nulmeting uitgevoerd aan de hand van <enquêtes en interviews>. Hieruit blijkt dat het huidige kennisniveau van medewerkers <hoog/gemiddeld/laag> is. Daarnaast heeft <naam schoolbestuur> de belangrijkste risico's in kaart gebracht rond digitaal veilig gedrag. De grootste risico's zijn:

* <Beschrijf de risico's.>
* Voorbeeld 1: Medewerkers melden incidenten niet.
* Voorbeeld 2: Medewerkers vergrendelen hun beeldscherm niet bij het verlaten van hun werkplek of de klas.
* Voorbeeld 3: Medewerkers hanteren zwakke wachtwoorden of delen hun wachtwoord met anderen.

# Het bewustwordingsprogramma

## Scope en strategie

***Toelichting***

* *Omschrijf de scope en strategie van het bewustwordingsprogramma. Koppel deze aan de nulmeting en de risico's.*
* *Koppel de scope van het bewustwordingsprogramma aan de doelgroep en de doelen.*

Het bewustwordingsprogramma van <naam schoolbestuur> is gericht op het creëren van een omgeving waarin de eigen verantwoordelijkheid van medewerkers voorop staat en waarin incidenten worden besproken en lessen worden geleerd. De medewerker staat centraal. Dit betekent dat we meerdere doelgroepen onderscheiden en dat we per doelgroep bewustwordingsmiddelen inzetten die passen bij de kennis, het gedrag en de verantwoordelijkheid van de medewerker. Bij het ontwikkelen of inkopen van bewustwordingsmiddelen wegen we inzichten uit de gedragswetenschap mee.

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.

## Doelgroep

***Toelichting***

* *Omschrijf de doelgroep van het bewustwordingsprogramma. Bepaal op basis van de grootste risico's wie de doelgroep is. Hoe gaan zij om met ICT en informatie en wat hebben zij nodig om digitaal veilig te werken? Welke gedragsverandering wil je zien? Welke factoren hebben hier invloed op? En hoe kun je mensen het makkelijker maken om het juiste gedrag te vertonen?*

Het bewustwordingsprogramma van <naam schoolbestuur> is gericht op:

1. <Doelgroep 1. Bijvoorbeeld: Medewerkers van het bestuurskantoor en OOP> De grootste uitdaging voor deze doelgroep is: <vul uitdaging(en) in>.
2. <Doelgroep 2. Bijvoorbeeld: Bestuurders en schoolleiders> De grootste uitdaging voor deze doelgroep is: <vul uitdaging(en) in>.
3. <Doelgroep 3. Bijvoorbeeld: Leraren/docenten>. De grootste uitdaging voor deze doelgroep is: <vul uitdaging(en) in>.
4. <Doelgroep 4. Bijvoorbeeld: Leerlingen> De grootste uitdaging voor deze doelgroep is: <vul uitdaging(en) in>.

## Doelstelling

***Toelichting***

* *Bepaal wat je met je bewustwordingsprogramma wilt bereiken. Koppel de doelen van het programma aan de risico's die je voor jouw organisatie ziet op het gebied van IBP. Kies doelen die gericht zijn op kennis, houding en gedrag en die rekening houden met de individuele (start)situatie van de medewerker. Heb je bij 2.2 meerdere doelgroepen omschreven? Beschrijf dan per doelgroep welke doelstelling(en) je wilt behalen.*
* *Bepaal of je schoolbestuur zich conformeert aan een concreet streefniveau en neem dit op in de doelstelling.*
* *Een bewustwordingsprogramma kan verschillende thema's hebben.*

*Drie voorbeelden van thema's zijn:*

* + *herkennen van dingen die niet in de haak zijn*
	+ *melden van dingen die misgaan*
	+ *digitaal veilig gedrag*

*Kies een thema en omschrijf hier concrete doelen bij. Bij digitaal veilig gedrag hoort bijvoorbeeld sterke wachtwoorden kiezen, een wachtwoordmanager gebruiken, wachtwoorden niet delen met anderen en het scherm vergrendelen bij het verlaten van de werkplek. Wees zo concreet mogelijk in het beschrijven van het gewenste gedrag en realiseer je dat niet iedereen altijd een phishingmail herkent. Dit kun je dus niet als gewenst gedrag formuleren.*

Het bewustwordingsprogramma van <naam schoolbestuur> is erop gericht om <doelgroep 1> bewust te maken van:

* <thema bewustwordingsprogramma>

Dit doen we concreet door:

* <bewustwordingsdoelen en onderwerpen voor afzonderlijke onderdelen van het programma>

Uit de nulmeting blijkt dat het huidige kennisniveau van deze doelgroep <hoog/gemiddeld/laag> is. Het streefdoel is <streefniveau>.

Het bewustwordingsprogramma van <naam schoolbestuur> is erop gericht om <doelgroep 2> bewust te maken van:

* <thema bewustwordingsprogramma>

Dit doen we concreet door:

* <bewustwordingsdoelen en onderwerpen voor afzonderlijke onderdelen van het programma>

## Bewustwordingsmiddelen en planning

***Toelichting***

* *Omschrijf de bewustwordingsmiddelen die je inzet binnen het programma en omschrijf hoe deze bijdragen aan het behalen van de gestelde doelen. Kies voor middelen die werken en maak hiervoor gebruik van inzichten uit de gedragswetenschappen. Je kunt zelf bewustwordingsmiddelen ontwikkelen of inkopen bij een leverancier. Op de deelprojectpagina vind je voorbeelden van publieke bewustwordingsmiddelen die je kunt inzetten. Maak ook een planning.*
* *Stem de middelen af op de doelgroep en maak een combinatie van digitale een fysieke middelen. Kies voor middelen die goed gedrag stimuleren en gericht zijn op beloning. Voorbeelden van bewustwordingsmiddelen zijn:*
	+ *medewerkersbijeenkomsten*
	+ *online informatie delen via webinars, podcasts, filmpjes en games*
	+ *interne communicatiemiddelen. Denk aan digitale middelen zoals berichten op het intranet of nieuwsbriefberichten en fysieke middelen zoals posters, stickers of tafelkalenders*
	+ *serious gaming zoals een crisisoefening*
	+ *eenmalige of terugkerende e-learning of micro-learning. Dit is een verkorte vorm van*

*e-learning.*

|  |
| --- |
| ***Valkuilen phishingtesten****Naast bovenstaande middelen worden soms ook phishingtesten en phishingsimulaties ingezet voor bewustwording. Wij raden scholen niet aan om dit middel in te zetten. Het is voor hackers laagdrempelig en goedkoop om grote aantallen phishingmails te versturen. Alleen als alle medewerkers iedere phishingmail op ieder moment herkennen is menselijke detectie een effectieve maatregel. Dit is in de praktijk onhaalbaar en daarom is dit bewustwordingsmiddel onvoldoende effectief. Technische maatregelen die voorkomen dat phishingmails medewerkers bereiken, bieden wel effectieve bescherming tegen deze phishingaanvallen.*  |

Voor het bewustwordingsprogramma zetten we de volgende middelen in die bijdragen aan de volgende doelen:

|  |  |  |  |
| --- | --- | --- | --- |
| **Doelgroep** | **Bewustwordings-middel** | **Draagt bij aan** | **Planning** |
| *<*Bijvoorbeeld bestuurders en schoolleiders en medewerkers crisisteam>   | *<*Bijvoorbeeld crisisoefening>  | *<*Bijvoorbeeld bewustzijn rol en verantwoordelijkheid bij crisis*>*   | <Bijvoorbeeld Q1>   |
| *<*Bijvoorbeeld leraren*>*  | *<*Bijvoorbeeld medewerkersbijeenkomst>  | *<*Bijvoorbeeld vergrendelen van beeldscherm bij verlaten werkplek*>*  | <Bijvoorbeeld Q1>  |
| *<*Bijvoorbeeld medewerkers*>*   | *<*Bijvoorbeeld micro-learnings>   | *<*Bijvoorbeeld melden van incidenten of datalekken>   | <Bijvoorbeeld Q2>  |
| *<*Bijvoorbeeld leerlingen*>*   | *<*Bijvoorbeeld game voor po-leerlingen>   | *<*Bijvoorbeeld gevolgen hacking>   | <Bijvoorbeeld Q4>   |
| <…>   | <…>   | <…>   | <…>   |

# Effect meten, evalueren en verbeteren

***Toelichting***

* *Omschrijf hoe je het effect van het bewustwordingsprogramma meet en hoe vaak je dit doet, hoe je het programma evalueert en hoe vaak, en hoe je het programma verbetert. Hanteer uitgangspunten die gerelateerd zijn aan de risico's die je hebt gesignaleerd en die gekoppeld zijn aan de doelstellingen van het programma.*
* *Heb je bewustwordingsmiddelen ingekocht bij een leverancier? Die hoort het effect van de middelen te meten en je daar inzicht in te geven.*

<Naam schoolbestuur> evalueert elke <aantal maanden> het bewustwordingsprogramma door middel van indicatoren, evaluatiesessies en gesprekken met betrokkenen. We hanteren daarbij de volgende indicatoren als uitgangspunten:

* <hanteer uitgangspunten die gerelateerd zijn aan de risico's die je hebt gesignaleerd en die gekoppeld zijn aan de doelstellingen>
* Voorbeeld 1: het aantal datalekken dat wordt gemeld.
* Voorbeeld 2: het aantal meldingen van beveiligingsincidenten in een bepaalde periode.
* Voorbeeld 3: het aantal computers waarvan bij een verlaten werkplek het scherm niet is vergrendeld.
* Voorbeeld 4: het aantal apparaten (laptops, smartphones, USB-sticks) dat als verloren of gestolen is gemeld.
* Voorbeeld 5: het aantal keren dat een phishingmail als beveiligingsincident wordt gemeld.

Uit deze evaluatie komen verbeterpunten naar voren voor het bewustwordingsniveau en voor thema's die extra aandacht verdienen. Deze thema's nemen we mee in de volgende cyclus van het programma. Daarnaast komen uit de evaluatie verbeterpunten voor het bewustwordingsprogramma zelf. Aan de hand van deze verbeterpunten passen we het programma aan. Zo wijzigen we de inzet van communicatiemiddelen per doelgroep wanneer deze niet goed op elkaar blijken aan te sluiten.