INTERACTIEVE HANDREIKING: STUREN OP DIGITALE VEILIGHEID

Informatiebeveiliging en Privacy in de Jaarcyclus

Versie: december 2024

PO RAAD VO RAAD Bit by Bit Samen voor digitaal veilig onderwijs

INLEIDING

Deze handreiking is een hulpmiddel voor bestuurders en beleidsmedewerkers om informatiebeveiliging en privacy (IBP) integraal op te nemen in de beleids- en uitvoeringscyclus van de organisatie. Denk aan de jaarplan- en begrotingscyclus. Het thema krijgt een plek op operationeel, tactisch én strategisch niveau. Zo komt IBP op vaste momenten op de (bestuurlijke) agenda en houd je regie op digitale veiligheid.

RISICOMANAGEMENT

De risico's op het gebied van cyberdreigingen en privacy in het onderwijs nemen toe. Met behulp van het **Dreigingsbeeld Funderend Onderwijs** krijg je een beter beeld van de dreigingen en risico's van jouw organisatie. Dit kun je vertalen naar je eigen organisatie en neem je mee in het integrale risicomanagement. Is IBP al een vast onderdeel van jullie risicomanagementproces? Heb je al crisismanagement ingericht? Neem je IBP mee in het integrale veiligheidsbeleid?

NORMENKADER IBP

Met behulp van het **Normenkader Informatiebeveiliging en Privacy** (Normenkader IBP) kun je kijken waar je organisatie staat. Ook vind je normen en maatregelen om de digitale veiligheid te verhogen en te voldoen aan wet- en regelgeving, waaronder de Algemene Verordening Gegevensbescherming (AVG). Zo borg je de digitale veiligheid en privacy van leerlingen en medewerkers en bescherm je je organisatie zo goed mogelijk tegen cyberincidenten.

BEWUSTWORDING EN PROFESSIONALISERING

Met het integraal opnemen van IBP in de beleids- en uitvoeringscyclus van je organisatie ben je er nog niet. Naast governance, beleid en processen zijn ook bewustwording en gedrag belangrijk. Informatiebeveiliging en privacy raakt iedereen in de organisatie. Denk aan bewustwording en professionalisering van alle medewerkers, inclusief de bestuurder(s) en de leden van de RvT. Ook voor leerlingen is digitale veiligheid een belangrijk aandachtspunt en maakt onderdeel uit van digitale geletterdheid. Zo weten medewerkers én leerlingen hoe zij veilig kunnen omgaan met systemen en informatie.

VOLGENDE:
LEMNISCAAT

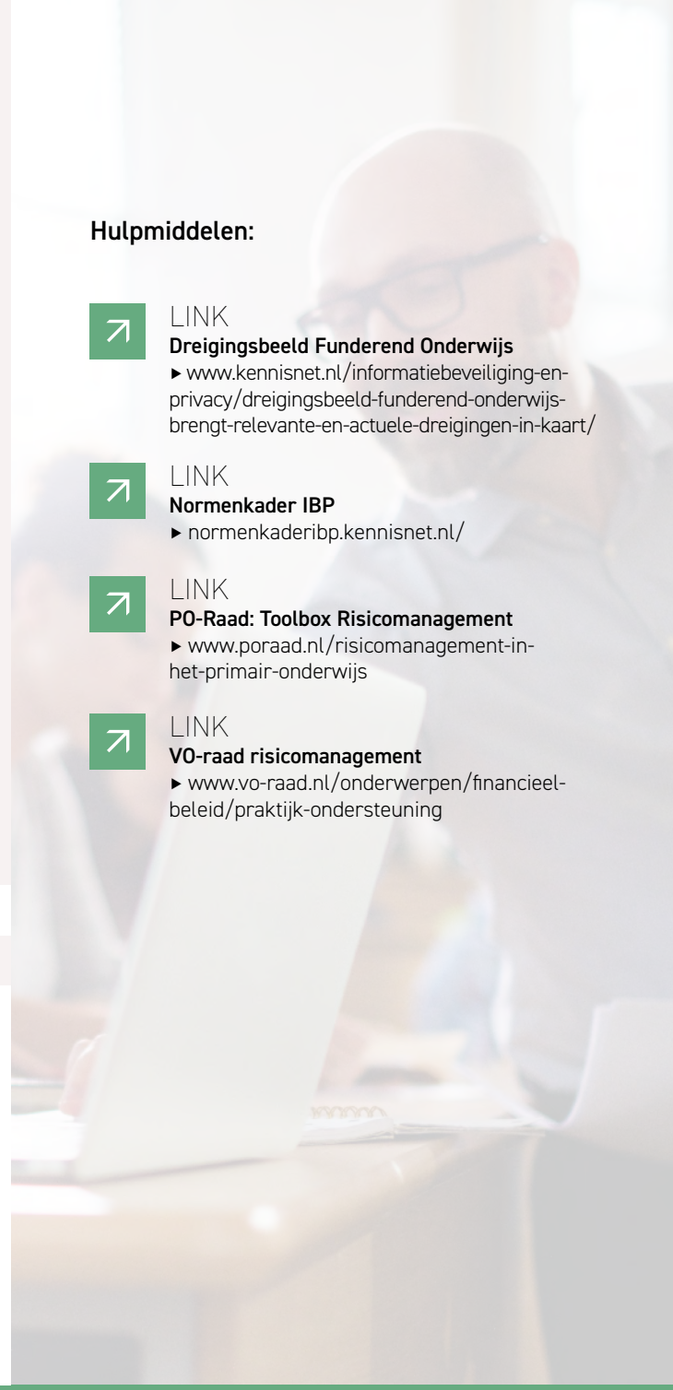
Hulpmiddelen:

LINK
Dreigingsbeeld Funderend Onderwijs
▸ www.kennisnet.nl/informatiebeveiliging-en-privacy/dreigingsbeeld-funderend-onderwijs-brengt-relevante-en-actuele-dreigingen-in-kaart/

LINK
Normenkader IBP
▸ normenkaderibp.kennisnet.nl/

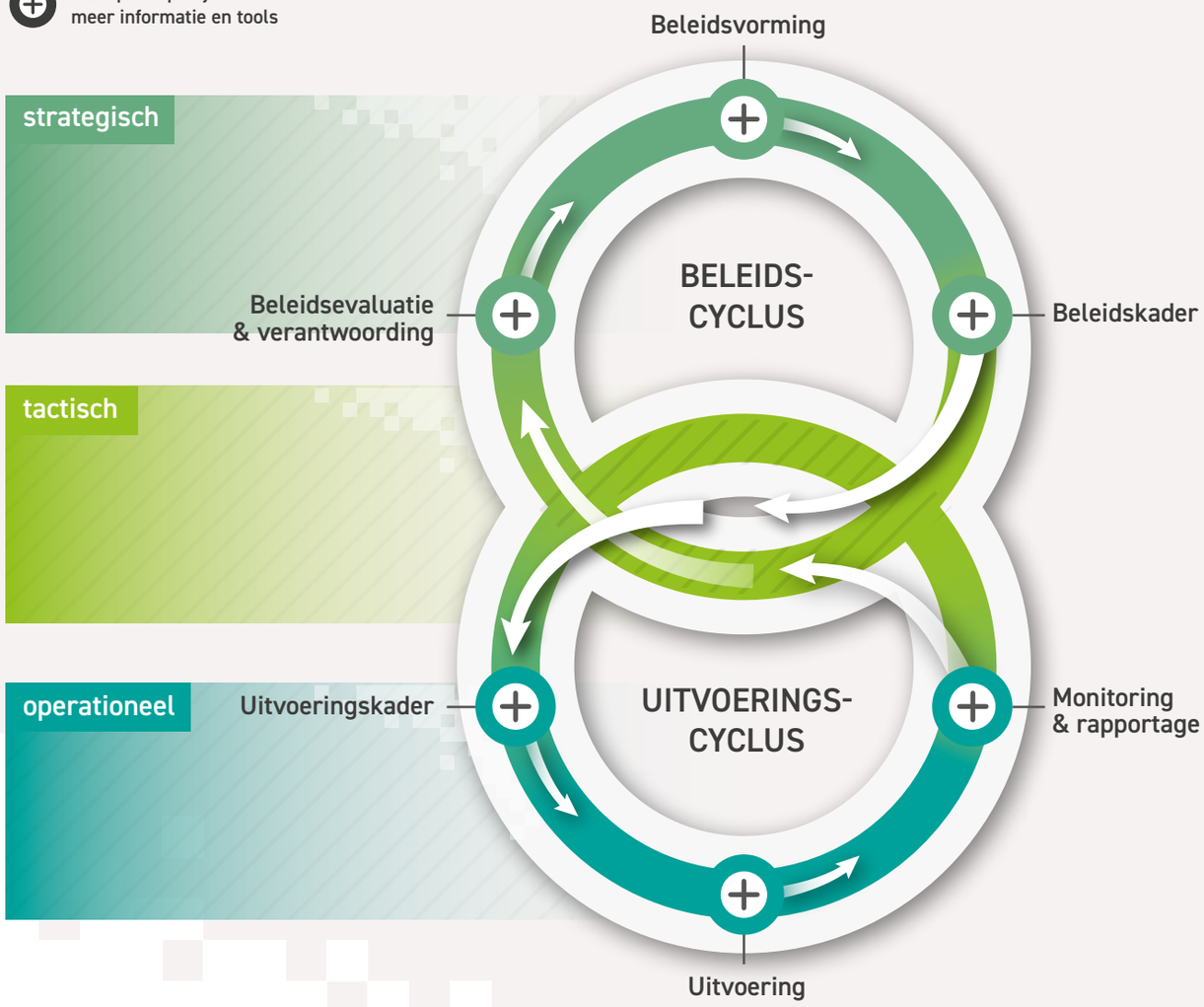
LINK
PO-Raad: Toolbox Risicomanagement
▸ www.poraad.nl/risicomanagement-in-het-primair-onderwijs

LINK
VO-raad risicomanagement
▸ www.vo-raad.nl/onderwerpen/financieel-beleid/praktijk-ondersteuning



LEMNISCAAT INFORMATIEBEVEILIGING EN PRIVACY IN DE JAARCYCLUS

klik op een plusje voor meer informatie en tools



STUREN OP DIGITALE VEILIGHEID

DOEL:
Het schoolbestuur heeft de regie op informatiebeveiliging en privacy in de organisatie.

HOE?
IBP onderdeel maken van de integrale beleids- en uitvoeringscyclus, zodat je weet of je in control bent en blijft en je kunt bijsturen.

HULPMIDDEL:
De interactieve handreiking 'Sturen op digitale veiligheid' helpt bestuurders om regie te pakken op informatiebeveiliging en privacy.

IBP is onderdeel van de cyclus van beleid, begroten, rapporteren en verantwoorden.

Op strategisch, tactisch en operationeel niveau.

Naast structuur zijn leiderschap en gedrag van belang voor succes.

BELEIDSVORMING

Welke ambitie heb je als schoolbestuur als het gaat om digitale veiligheid en hoe ga je aan de slag met het Normenkader IBP? In de stap beleidsvorming bespreek je visie en strategie met belanghebbenden, leg je vast wanneer het bestuur betrokken wordt en beleg je IBP-rollen en verantwoordelijkheden.

Visie en strategie
Een **visie en strategie** zijn leidend voor hoe je organisatie omgaat met informatiebeveiliging en privacy. Welke ambitie heb je als schoolbestuur als het gaat om digitale veiligheid, waarom en hoe wil je die bereiken? Deze visie en strategie vormen de basis voor het IBP-beleid dat je ontwikkelt in de volgende stap 'beleidskader'. Bespreek de visie en strategie ook met je **interne stakeholders** waaronder de RvT, (G)MR, schoolleiders en managers (ICT, HR, facilitair, bedrijfsvoering en financiën).

Betrokkenheid bestuur
Een hoge betrokkenheid van de bestuurder resulteert in een hogere mate van volwassenheid van de organisatie op het gebied van informatiebeveiliging en privacy. Het bestuur is **eindverantwoordelijk** en geeft richting aan de organisatie. Welke besluiten neem je op **strategisch**, **tactisch en operationeel niveau**? Wanneer moet de bestuurder betrokken worden en welk mandaat krijgen medewerkers? Zijn er afspraken gemaakt over **monitoring** van de **voortgang** en evaluatie?

Rollen en verantwoordelijkheden
Tijdens de beleidsvorming wijs je formeel **eigenaarschap, rollen, verantwoordelijkheden** toe. Is er een privacy en/of security officer? Is er een FG (functionaris gegevensbescherming) en een CISO (Chief Information Security Officer)? Welke rol en verantwoordelijkheid krijgen schoolleiders en managers (denk aan hoofd ICT, HR, facilitair, bedrijfsvoering en financiën)? De keuzes over het beleggen van IBP-rollen en verantwoordelijkheden geef je een plek in het IBP-beleid.

Kernwoorden: visie en strategie, interne stakeholders, rollen en verantwoordelijkheden.

Mijlpaal: visie en strategie is ontwikkeld en verantwoordelijkheden zijn toegewezen.

VOLGENDE:
BELEIDSKADER

Hulpmiddelen:

LINK
Groeipad: Fase 1 - Deelproject Beleid, strategie en verantwoordelijkheden
https://normenkaderibp.kennisnet.nl/groeipad/fase-1/

BELEIDSKADER

In de vorige stap 'beleidsvorming' is de organisatiebrede visie en strategie opgesteld en zijn rollen en verantwoordelijkheden belegd. Dit is de basis voor het **IBP-beleid**. In de stap beleidskader ontwikkelen de hiervoor aangewezen IBP-medewerkers het IBP-beleid voor de organisatie. Dit beleid wordt vastgesteld door het schoolbestuur en wordt breed gecommuniceerd binnen de organisatie.

Data en informatie
Heb je zicht op de volwassenheid van de organisatie ten opzichte van het Normenkader IBP? Is er al een **nulmeting** of **risicoanalyse** gemaakt? Deze **data en informatie** zijn input voor het opstellen of actualiseren van het IBP-beleid. Wat zijn (nog) risico's en kwetsbaarden voor de organisatie? Welke maatregelen wil je nemen?

Betrokkenheid medewerkers
Bespreek het (te ontwikkelen) IBP-beleid met collega's die een rol en verantwoordelijkheid hebben, waaronder schoolleiders en managers op het gebied van ICT, HR, facilitair, bedrijfsvoering en financiën. Hoe raken de IBP-doelstellingen hun domein of hun school? Hoe kunnen zij in de komende periode bijdragen aan de doelen en het uitdragen van het beleid richting de medewerkers? Welke doelen en maatregelen hebben invloed op de hele organisatie en welke op schoolniveau?

Kernwoorden: IBP-beleid, data en informatie.

Mijlpaal: IBP-beleid is ontwikkeld en medewerkers in de organisatie zijn betrokken en/of geïnformeerd.

VOLGENDE:
UITVOERINGSKADER

Hulpmiddelen:

LINK
Groeipad: Fase 1 - Deelproject Beleid, strategie en verantwoordelijkheden
https://normenkaderibp.kennisnet.nl/groeipad/fase-1/

LINK
Toolbox bekostiging en begroting | PO-Raad
▸ www.poraad.nl/arbeidszaken-bedrijfsvoering/financien-primair-onderwijs/toolbox-bekostiging-en-begroting

LINK
Toolbox begroting | VO-raad
▸ www.vo-raad.nl/onderwerpen/financieel-beleid/praktijk-ondersteuning

UITVOERINGSKADER

In de vorige stap is het IBP-beleid opgesteld. In de stap uitvoeringskader vertaal je visie, strategie en beleid naar een concrete **roadmap/planning**. Zo weet je wat je de komende jaren gaat doen. Wat is er nodig om werk te maken van de maatregelen uit het Normenkader IBP? Met welke normen begin je? Volg je het **Groeipad** of heb je een eigen aanpak voor je bestuur opgesteld?

Jaarplan en begroting
Je weet nu wat je komend jaar precies gaat doen en maakt een inschatting wat dit vraagt van de organisatie. Neem het thema IBP integraal op in het organisatiebrede **jaarplan** en de **begroting**. Het thema krijgt immers ook een vaste plek in het jaarverslag.
Hoeveel fte en financiële middelen zijn er nodig om de ambitie en doelstellingen te realiseren? En is er voldoende budget vrijgemaakt of moeten er nog keuzes gemaakt worden? Het jaarplan en de begroting worden vastgesteld door het schoolbestuur.

Professionalisering
Om aan de slag te gaan is het van belang dat er medewerkers zijn aangewezen met voldoende kennis en vaardigheden en voldoende tijd om dit op te pakken. Is er aandacht voor hun **professionalisering**? Zijn ze lid van het **Netwerk IBP**?

Kernwoorden: roadmap, planning, jaarplan, begroting, groeipad, professionalisering.

Mijlpaal: het uitvoeringskader (roadmap/planning) is vastgesteld en vertaald naar een jaarplan en begroting.

VOLGENDE:
UITVOERING

Hulpmiddelen:

LINK
Groeipad
▸ normenkaderibp.kennisnet.nl/groeipad/

LINK
Netwerk IBP
▸ aanpakibp.kennisnet.nl/netwerk-informatiebeveiliging-en-privacy/

UITVOERINGSKADER
UITVOERING
MONITORING & RAPPORTAGE
operationeel

UITVOERING

In de vorige stap is het uitvoeringskader (roadmap/planning en jaarplan inclusief begroting) vastgesteld. De medewerkers die verantwoordelijk zijn voor de uitvoering van de maatregelen uit het Normenkader IBP gaan nu aan de slag. Op de website van het Normenkader IBP is **ondersteuningsaanbod** te vinden waaronder het Groeipad, uitleg om aan de slag te gaan en voorbeelddocumenten.

In de praktijk
Zijn de rollen en verantwoordelijkheden op operationeel niveau duidelijk? Wie heeft welk mandaat om besluiten te nemen in de uitvoering? Is er sprake van **eigenaarschap** bij de medewerkers die niet direct betrokken zijn bij het thema IBP (zoals schoolleiders of managers) maar wel een rol of verantwoordelijkheid hebben? Besteedt de organisatie aandacht aan **bewustwording** van alle medewerkers, naast procesverbetering en technische maatregelen?

Voortgang
Hoe houd je zicht op de **voortgang**? Gebruik je als organisatie bijvoorbeeld een Excel-spreadsheet of (GRC-)tooling om de voortgang bij te houden?

Kernwoorden: uitvoering, eigenaarschap, bewustwording, voortgang.

Mijlpaal: mijlpalen binnen het uitvoeringsplan behaald.

Hulpmiddelen:

LINK
Hulpmiddelen normenkader
▸ normenkaderibp.kennisnet.nl/hulpmiddelen/

LINK
Groeipad
▸ normenkaderibp.kennisnet.nl/groeipad/

LINK
(GRC-)tooling
▸ sivon.nl/governance-risk-compliance-grc/

VOLGENDE:
MONTORING & RAPPORTAGE

UITVOERING
operationeel
MONITORING & RAPPORTAGE
BELEIDSEVALUATIE & VERANTWOORDING

MONITORING & RAPPORTAGE

Hoe toets je waar de organisatie staat ten opzichte van het normenkader? Met een **self-assessment, een interne of externe audit**? Doe je mee aan een deep dive workshop? Met onafhankelijke toetsing krijg je in beeld waar de dagelijkse praktijk afwijkt van het beleid en de procedures.

Laat het **auditplan** vaststellen door het schoolbestuur of een auditcommissie. In een **interne auditcommissie** zitten bijvoorbeeld de bestuurder, een schoolleider, manager/hoofd bedrijfsvoering en lid RvT. Zij beoordelen of de organisatie voldoende in control is.

Nieuw: vanaf maart 2025 kunnen schoolbesturen meedoen aan de Monitor Digitalisering Onderwijs. Met de monitor krijgen scholen inzicht in waar ze zelf staan op het gebied van digitalisering én kunnen ze zichzelf vergelijken met het landelijk gemiddelde. Informatiebeveiliging en privacy (IBP) is een apart thema binnen de monitor.

Kernwoorden: self-assessment, interne of externe audit.

Mijlpaal: auditplan vastgesteld, toetsing uitgevoerd.

Hulpmiddelen:

LINK
Auditplan normenkader
▸ normenkaderibp.kennisnet.nl/informatiebeveiliging/domein-1-bestuur/go-05-onafhankelijke-toetsing/

LINK
deep dive workshop
▸ sivon.nl/deep-dive/

LINK
PO-Raad: Monitor Digitalisering Onderwijs
▸ https://www.poraad.nl/schoolontwikkeling/digitalisering/monitor-digitalisering-onderwijs-0

LINK
VO-raad: Monitor Digitalisering Onderwijs
▸ https://www.vo-raad.nl/onderwerpen/digitalisering/data-over-digitalisering#sectorrapportage

VOLGENDE:
BELEIDSEVALUATIE & VERANTWOORDING

BELEIDSEVALUATIE & VERANTWOORDING

Op basis van de informatie uit een monitor en/of (interne of externe) audit evalueer je waar het schoolbestuur staat en leg je daar **verantwoording** over af aan interne en eventueel externe stakeholders.

Evaluatiegesprekken
Voer jaarlijks gesprekken met stakeholders op basis van een (audit-) rapportage of jaarverslag, denk aan de RvT, (G)MR, schoolleiders en managers (ICT, HR, facilitair, bedrijfsvoering en financiën). Ook schoolleiders en leidinggevenden kunnen het onderwerp meenemen in de **jaarlijkse gesprekscyclus** met medewerkers. De uitkomsten uit deze gesprekken zijn input voor een evaluatie waarmee je kunt afwegen of het huidige IBP-beleid nog actueel is.

Bestuursverslag
Vanaf 2024 is het verplicht om Informatiebeveiliging en Privacy op te nemen in het **bestuursverslag**. Het bestuursverslag en de rapportage van de **accountant** zijn jaarlijks terugkerende onderwerpen op de agenda. Betrek de IBP-medewerker of FG bij het opstellen van het jaarverslag. Gebruik deze momenten als haakje om ook informatiebeveiliging en privacy te bespreken met het bestuur en de RvT.

Kernwoorden: evaluatie en verantwoording, jaarlijkse gesprekken.

Mijlpalen: IBP is onderdeel van het bestuursverslag, evaluatiegesprekken uitgevoerd.

VOLGENDE:
COLOFON

Hulpmiddelen:

LINK
Handreiking voor bestuursverslag
▸ https://normenkaderibp.kennisnet.nl/privacy/domein-7-verantwoording/

LINK
Handreiking voor bestuursverslag 2023 | VO-raad
▸ www.vo-raad.nl/nieuws/handreiking-voor-bestuursverslag-2023

LINK
Handreiking: de rol van de RvT bij Digitale Veiligheid
▸ https://www.vo-raad.nl/handreikingrvtdigitaleveiligheid

LINK
Bestuursverslag PO-raad 2023
▸ https://www.poraad.nl/vernieuwde-handreiking-voor-bestuursverslag-beschikbaar

BELEIDSEVALUATIE & VERANTWOORDING
BELEIDSVORMING
BELEIDSKADER
strategisch

→ COLOFON

Versie: december 2024

De Interactieve handreiking ‘Sturen op Digitale Veiligheid’ is ontwikkeld door de PO-Raad en VO-raad in samenwerking met Kennisnet, als onderdeel van programma Digitaal Veilig Onderwijs.

Digitaal Veilig Onderwijs:
Met het programma Digitaal Veilig Onderwijs bundelen het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en VO-raad hun krachten voor een onderwijssector waarin iedere leerling digitaal veilig kan leren en medewerkers digitaal veilig kunnen werken. Het programma biedt schoolbesturen en leveranciers heldere leidraden en een concreet ondersteuningsaanbod. Zo kunnen zij voldoen aan hun verantwoordelijkheid om een digitaal veilige organisatie te realiseren. Stap voor stap, Bit by Bit.

Met speciale dank aan:
De leden van de Klankbordgroep Digitale Veiligheid (PO-Raad en VO-raad).

Levend document
Kennisnet werkt momenteel aan een doorontwikkeling van het Groeipad en de hulpmiddelen behorend bij het Normenkader IBP. Deze handreiking is een levend document. Wij actualiseren regelmatig de informatie en links naar relevante hulpmiddelen. Kijk daarom of je de meest recente versie voor je hebt.

INTERACTIEVE HANDREIKING:
STUREN OP DIGITALE VEILIGHEID

Informatiebeveiliging en Privacy in de Jaarcyclus

Versie: december 2024

PO RAAD VO RAAD Bit by Bit Samen voor digitaal veilig onderwijs