

Fysiek beveiligingsbeleid

Voorbeelddocument

Versie: Mei 2025



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

**Over dit voorbeelddocument**

**Dit voorbeelddocument helpt je met het maken van een eigen beleid voor fysieke beveiliging. 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 beleid definitief maakt.
* Dit beleid gaat ervan uit dat taken, rollen en functies die nodig zijn om het beleid op te stellen en 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](#_Toc197583830)

[1.1 Doel 5](#_Toc197583831)

[1.2 Reikwijdte 5](#_Toc197583832)

[2 Uitgangspunten 6](#_Toc197583833)

[2.1 Zonering 6](#_Toc197583834)

[2.2 Toegangsrechten 6](#_Toc197583835)

[2.3 Fysieke beveiliging 7](#_Toc197583836)

[2.4 Bescherming van netwerkvoorzieningen 7](#_Toc197583837)

[2.5 Cameratoezicht 7](#_Toc197583838)

# Inleiding

***Toelichting***

* *In dit hoofdstuk geef je aan wat de doelen van het fysieke beveiligingsbeleid zijn. De hiervoor geformuleerde doelen zijn voorbeelden. Pas ze aan aan je eigen organisatie.*
* *Binnen dit hoofdstuk bepaal je ook de reikwijdte van het fysieke beveiligingsbeleid. Om te voldoen aan het Normenkader IBP moet het in elk geval gaan over ruimtes waarin persoonsgegevens worden opgeslagen of verwerkt en IT-ruimtes. Daarnaast kun je specificeren voor welke locaties van je organisatie dit beleid geldt. Heb je al een beleid voor fysieke beveiliging in je organisatie? Dan kun je ervoor kiezen om de uitgangspunten daarin op te nemen.*

## Doel

Fysieke toegang tot netwerken, systemen en gegevens door onbevoegden levert een bedreiging op voor de vertrouwelijkheid, beschikbaarheid en integriteit van de informatie en informatieverwerking van <vul naam organisatie in>. Met behulp van maatregelen voor fysieke beveiliging worden deze risico’s beperkt.

## Reikwijdte

Het fysieke beveiligingsbeleid is van toepassing op alle medewerkers, leerlingen en bezoekers van <vul naam organisatie in>. Dit beleid is van toepassing op de volgende locaties:

* <Vul locaties aan>

# Uitgangspunten

***Toelichting***

* *In dit hoofdstuk geef je aan hoe de fysieke beveiliging binnen je organisatie is georganiseerd. Welke algemene maatregelen zijn er en welke specifieke maatregelen zijn er voor specifieke zones?*
* *In dit voorbeelddocument maken we gebruik van drie zones. Je kunt gebruikmaken van een andere zonering of indeling. Bij de zones zijn voorbeelden beschreven van de ruimtes.*
* *In dit voorbeelddocument beschrijven we enkele voorbeeldmaatregelen. Beschrijf de maatregelen voor fysieke beveiliging die worden genomen op basis van de risicoanalyse voor je fysieke beveiliging.*

## Zonering

Ten behoeve van de beveiliging van informatie, is er een toegangsbeleid voor alle voorzieningen van <vul naam organisatie in>. In dit beleid onderscheiden we diverse beveiligingszones:

|  |  |
| --- | --- |
| Zone 0 | In de hal is een receptie, deze is openbaar toegankelijk.  |
| Zone 1 | De klaslokalen, fietsenstalling, aula en andere ruimtes die toegankelijk zijn voor leerlingen en medewerkers.  |
| Zone 2 | Dit betreft zones die uitsluitend bereikbaar zijn met toegangspassen of sleutels voor geautoriseerde medewerkers, zoals: * Kantoorwerkplekken,
* Lerarenkamer.
 |
| Zone 3 | Er zijn ondersteunende ruimtes, waarvan de toegang wordt geregeld met een sleutelplan of een elektronische toegangsbeveiliging en alarmering. Het gaat om: * Archieven,
* Server- en netwerkruimtes,
* Off-site back-uplocatie.
 |

## Toegangsrechten

* Toegang tot beveiligingszones is alleen mogelijk na autorisatie.
* Medewerkers/bezoekers zonder autorisatie mogen alleen onder begeleiding van bevoegd personeel en als er een noodzaak is toegang krijgen tot de beveiligde omgeving.
* Er wordt gebruikgemaakt van toegangspassen. Deze vallen onder de verantwoordelijkheid van de administratie.
* De verantwoordelijke voor personeelszaken informeert de facilitaire dienst over vertrekkende en nieuwe medewerkers, waarop de administratie fysieke toegangsrechten aanpast.
* Er vindt één keer per halfjaar een controle/evaluatie plaats op de autorisaties voor fysieke toegang. Voor speciale toegangsrechten in zone 3 is dat minimaal ieder kwartaal.

## Fysieke beveiliging

* Vertrouwelijke ruimtes zijn afgesloten met sleutels, waarvoor de administratie een sleutelplan heeft opgesteld.
* Maatregelen voor brandveiligheid zijn in lijn met het bouwbesluit.
* Voor de off-site back-uplocatie zijn aanvullende fysieke beveiligingsmaatregelen genomen, te weten:
	+ <invullen indien relevant>

## Bescherming van netwerkvoorzieningen

* De toegang tot de patchkast en serverruimtes is beperkt tot in de autorisatiematrix aangewezen functies.
* Kabels die stroom, gegevens of ondersteunende informatiediensten vervoeren, worden beschermd tegen onderschepping, interferentie of schade.
* UTP-kabels zijn afgeschermd van stroomkabels om interferentie te voorkomen.
* Kabels t.b.v. *core-*connectiviteit (zoals glasvezel voor internettoegang) worden beschermd tegen ongeoorloofde fysieke toegang.

## Cameratoezicht

* Er is cameratoezicht op <beschrijf locaties met cameratoezicht>.
* Voorafgaand aan de inzet van cameratoezicht, is er een DPIA uitgevoerd, die staat vastgelegd in <vul in>.
* De (G)MR heeft ingestemd met het inzetten van cameratoezicht.
* Het reglement cameratoezicht beschrijft taken, verantwoordelijkheden en procedures over het cameratoezicht, met het oog op integer gebruik van het camerasysteem en de bescherming van privacy van leerlingen, medewerkers en bezoekers.