

BIV-classificatieproces

Voorbeelddocument

Versie: Maart 2025



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

**Over dit voorbeelddocument**

**Dit voorbeelddocument helpt je met het maken van een eigen BIV-classificatieproces. 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](#_Toc193985478)

[2 Processtappen 5](#_Toc193985479)

[2.1 Voorbereiden 5](#_Toc193985480)

[2.2 Uitvoeren BIV-classificatie 6](#_Toc193985481)

[2.3 Beveiligingsinstellingen bepalen en implementeren 6](#_Toc193985482)

[2.4 Monitoring 7](#_Toc193985483)

[3 Rollen en verantwoordelijkheden 7](#_Toc193985484)

# Inleiding

Het BIV-classificatieproces is bedoeld om gegevens en systemen op een passende manier te beschermen door middel van een BIV-classificatie en bijbehorende maatregelen. Deze procesbeschrijving beschrijft hoe dit wordt uitgevoerd binnen <vul naam organisatie in>. Dit proces sluit aan bij het IBP-beleid van <vul naam organisatie in>.

# Processtappen

Het BIV-classificatieproces bestaat uit 4 stappen waarbij we gebruikmaken van een risicogestuurde aanpak. Het uitvoeren van een BIV-classificatie, het toepassen van de juiste maatregelen en het monitoren van de effectiviteit van de geïmplementeerde maatregelen zorgen dat het juiste niveau van bescherming wordt toegepast voor de verschillende soorten systemen en gegevens. Het BIV-classificatieproces bestaat uit de volgende 4 processtappen:

* Voorbereiden
* Uitvoeren BIV-classificatie
* Maatregelen bepalen en implementeren
* Monitoren

Hieronder lichten we elke stap toe.

## Voorbereiden

***Toelichting***

* *Voordat je start met deze processtap is het nodig een BIV-classificatieschema vast te stellen die wordt gebruikt voor het uitvoeren van alle BIV-classificaties. Je kunt hiervoor het* [certificeringsschema IBP ROSA](https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa-v3-0/) *gebruiken.*
* *In het* [deelproject 1.6 Overzicht creëren van systemen en hardware](https://normenkaderibp-a.kennisnet.nl/groeipad/fase-1/deelproject-1-6-overzicht-creeren-van-systemen-en-hardware/) *worden systemen geregistreerd in een configuratiemanagementdatabase (CMDB). Gebruik het overzicht uit dat deelproject om te bepalen voor welk systeem de BIV-classificatie nog niet is uitgevoerd.*
* *Zorg dat in het leveranciers(risico)managementproces een verwijzing wordt opgenomen naar dit proces voor het uitvoeren van de BIV-classificatie voor nieuwe systemen.*
* *Het BIV-classificatieproces in dit voorbeelddocument bevat aspecten van het* [deelproject 2.7 Beveiligingseisen en maatregelen vastleggen in securitybaselines](https://normenkaderibp-a.kennisnet.nl/groeipad/fase-2/deelproject-2-7-beveiligingseisen-en-maatregelen-vastleggen-in-securitybaselines/)*. Wanneer je deze twee deelprojecten apart oppakt of het proces anders inricht, is het nodig het BIV-classificatieproces te beperken tot stappen 2.1 en 2.2.*
1. Bepaal welk systeem gaat worden geclassificeerd en leg vast wie die classificatie uitvoert in de BIV-classificatieschema.
2. De systeemeigenaar zorgt dat de proceseigenaren of andere vertegenwoordigers van de gebruikers van het systeem aanwezig zijn bij het classificeren.
3. De systeemeigenaar onderzoekt of de leverancier al een BIV-classificatie heeft uitgevoerd voor het betreffende systeem. Deze classificatie wordt gebruikt als vergelijkingsmateriaal tijdens het uitvoeren van de eigen BIV-classificatie. Ook verzamelt de systeemeigenaar andere bruikbare informatie, zoals de business-impactanalyses.

## Uitvoeren BIV-classificatie

***Toelichting***

* *Bepaal of het nodig is het classificatieniveau van een systeem ook in de CMDB op te nemen. Ga hiervoor naar het* [deelproject 1.6 Overzicht creëren van systemen en hardware](https://normenkaderibp-a.kennisnet.nl/groeipad/fase-1/deelproject-1-6-overzicht-creeren-van-systemen-en-hardware/)*.*
* *Het BIV-classificatieproces in dit voorbeelddocument bevat aspecten van het* [deelproject 2.7 Beveiligingseisen en maatregelen vastleggen in securitybaselines](https://normenkaderibp-a.kennisnet.nl/groeipad/fase-2/deelproject-2-7-beveiligingseisen-en-maatregelen-vastleggen-in-securitybaselines/)*. Wanneer je deze twee deelprojecten apart oppakt of je proces anders inricht, is het nodig het BIV-classificatieproces te beperken tot stappen 2.1 en 2.2.*
1. De systeemeigenaar voert samen met de betrokkenen uit stap 2.1B de BIV-classificatie uit, waarbij er een Laag (L), Midden (M) of Hoog (H) score wordt toegekend voor de Beschikbaarheid, Integriteit en Vertrouwelijkheid. Indien gewenst begeleidt de IBP’er deze processtap.
2. De systeemeigenaar legt de classificatie van het systeem vast in het BIV-classificatieschema.

## Beveiligingsinstellingen bepalen en implementeren

***Toelichting***

* *Bepaal of de maatregelen uit de securitybaseline worden opgenomen in het BIV-classificatieschema of dat een andere plek beter geschikt is om dit vast te leggen.*
* *Beschrijf hoe afwijkingen aan de baseline worden vastgelegd en wie deze uitzonderingen mag goedkeuren.*
1. Op basis van de BIV-classificatie uit stap 2.2 worden de juiste maatregelen uit de securitybaseline geselecteerd.
2. Afwijkingen van de maatregelen uit de securitybaseline (stap 2.3A) worden gemitigeerd met aanvullende maatregelen of formeel geaccepteerd door <functie>.
3. Maatregelen, afwijkingen en aanvullende maatregelen worden vastgelegd in het BIV-classificatieschema.
4. De betreffende medewerkers of leveranciers implementeren de maatregelen zoals vastgelegd in 2.3C.

## Monitoring

***Toelichting***

* *Beschrijf hoe de IBP’er monitort of de systemen nog in lijn met de securitybaseline zijn geconfigureerd.*
* *Beschrijf hoe afwijkingen worden behandeld en of er periodieke rapportages aan het management worden verschaft.*
1. De systeemeigenaar controleert de implementatie en toepassing van de maatregelen zoals vastgelegd in stap 2.3C.
2. De IBP’er voert <frequentie> een tweedelijnscontrole uit op de toepassing van de maatregelen zoals vastgelegd in stap 2.3C. Afwijkingen worden besproken met de betreffende systeemeigenaar en opgenomen in het incidentenregister.

# Rollen en verantwoordelijkheden

***Toelichting***

* *Vul het overzicht aan met de belegde rollen en verantwoordelijkheden.*

De volgende rollen zijn binnen <naam schoolbestuur> betrokken bij het risicomanagementproces.

|  |  |
| --- | --- |
| **Rol**  | **Verantwoordelijkheden** |
| **Eerste lijn** |
| Bestuur, directie, schoolleiding | * < Bepaal welke rol deze verantwoordelijkheid heeft: Goedkeuren van uitzonderingen op de securitybaseline.>
* <Vul aan met verantwoordelijkheden>.
 |
| Systeemeigenaar | * Uitvoeren van BIV-classificatie.
* Vastleggen van BIV-classificatie in CMDB.
* Controleren op implementatie en toepassing van de maatregelen.
* <Vul aan met verantwoordelijkheden>.
 |
| IT-medewerkers | * Implementeren maatregelen in lijn met securitybaseline.
* <Vul aan met verantwoordelijkheden>.
 |
| **Tweede lijn** |
| Proceseigenaar | * Opstellen en beheren van de BIV-classificatieprocesbeschrijving en het BIV-classificatieschema.
* <Vul aan met verantwoordelijkheden>.
 |
| IBP’er, CISO, security officer, privacy officer | * Periodiek controleren op de geïmplementeerde maatregelen.
* <Vul aan met verantwoordelijkheden>.
 |
| **Derde lijn** |
| Interne audit | * Bepaal of deze rol een functie heeft binnen dit proces.
* <Zo ja, vul aan met verantwoordelijkheden>.
 |