

Back-up en herstel van gegevens

Voorbeelddocument

Versie: April 2025



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

**Over dit voorbeelddocument**

**Dit voorbeelddocument helpt je met het maken van een eigen back-up en herstelproces. 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](#_Toc196378160)

[2 Processtappen 5](#_Toc196378161)

[2.1 Identificeren van kritieke systemen 5](#_Toc196378162)

[2.2 Vastleggen van maatregelen 6](#_Toc196378163)

[2.3 Toepassen van maatregelen 6](#_Toc196378164)

[2.4 Testen van herstel 6](#_Toc196378165)

[2.5 Monitoren van back-ups 7](#_Toc196378166)

[3 Rollen en verantwoordelijkheden 8](#_Toc196378167)

# Inleiding

Het back-up- en herstelproces zorgt ervoor dat belangrijke data op regelmatige basis veilig wordt opgeslagen. Ook zorgt dit proces ervoor dat kritieke systemen operationeel blijven bij onverwachte storingen of technische problemen. In het geval van verlies of beschadiging van gegevens, kan het systeem of de data snel worden hersteld, zodat de continuïteit van bedrijfsprocessen blijft gewaarborgd. Deze procesbeschrijving beschrijft hoe het back-up- en herstelproces wordt uitgevoerd binnen <vul naam organisatie in>.

# Processtappen

Het back-up- en herstelproces bestaat uit 5 stappen die er samen voor zorgen dat back-ups van data en systemen op een juiste manier zijn ingeregeld. Aan de hand daarvan zorgen we als organisatie voor de juiste beschikbaarheid van data en systemen. Bij uitval van systemen of verlies van data, zorgen we met dit proces voor een tijdig herstel. Het back-up- en herstelproces bestaat uit de volgende 5 processtappen:

* Identificeren van kritieke systemen
* Vastleggen van maatregelen
* Toepassen van maatregelen
* Testen van herstel
* Monitoren van back-ups

Hieronder lichten we elke stap toe.

## Identificeren van kritieke systemen

***Toelichting***

* *Voor het inrichten van dit proces is het nodig eerst de volgende deelprojecten uit te voeren: 1.6 Overzicht creëren van systemen en hardware, 1.7 Classificeren van systemen, 2.7 Beveiligingseisen en -maatregelen vastleggen in een beveiligingsbaseline en 2.10 Waarborgen van bedrijfscontinuïteit. Heb je dat nog niet gedaan? Ga daar dan eerst mee aan de slag.*
1. Maak een overzicht van de kritieke systemen op basis van de uitgevoerde BIV-classificaties en bedrijfsimpactanalyse.
2. Bij elk nieuw ingekocht of ontwikkeld systeem dient de beoordeling van stap 2.1A te worden uitgevoerd.

## Vastleggen van maatregelen

***Toelichting***

* *Voor het inrichten van dit proces is het nodig eerst de volgende deelprojecten uit te voeren: 1.6 Overzicht creëren van systemen en hardware, 1.7 Classificeren van systemen, 2.7 Beveiligingseisen en -maatregelen vastleggen in een beveiligingsbaseline en 2.10 Waarborgen van bedrijfscontinuïteit. Heb je dat nog niet gedaan? Ga daar dan eerst mee aan de slag.*
* *Bepaal of centrale vastlegging van back-upmaatregelen per systeem wenselijk is. Dit kun je doen door ‘ja/nee’ vast te leggen in de configuratiemanagementdatabase (CMBD). Hiermee creëer je een overzicht waardoor de tweede lijn gestructureerd controles kan uitvoeren zonder alle individuele BIV-classificaties te hoeven raadplegen.*
1. Leg in het CMDB per systeem vast of er back-upmaatregelen zijn vereist op basis van stap 2.1A.
2. Door middel van het BIV-classificatieproces, zijn er maatregelen voor back-up en herstel voorgeschreven. Bepaal per systeem welke back-upmaatregelen nodig zijn door gebruik te maken van dit proces en leg deze maatregelen vast in het BIV-classificatieschema. Leg per systeem vast of hersteltesten worden uitgevoerd en met welke frequentie.
3. Als een leverancier het systeem beheert, is het leveranciersrisicomanagementproces van toepassing.

## Toepassen van maatregelen

1. De systeemeigenaar zorgt dat de back-up- en herstelmaatregelen, zoals beschreven in de uitgevoerde BIV-classificatie, bij de juiste medewerker worden belegd.
2. De medewerker die verantwoordelijk is voor de uitvoering van de maatregelen, implementeert in overleg met de systeemeigenaar de maatregelen uit stap 2.2B. Zorg dat er een keuze wordt gemaakt over de opslag van back-ups op een andere fysieke locatie (offsite).

## Testen van herstel

***Toelichting***

* *Bepaal of centrale vastlegging van hersteltesten per systeem wenselijk is. Door een datum vast te leggen van de laatst uitgevoerde hersteltest in het CMDB, creëer je een overzicht waardoor de tweede lijn gestructureerd controles kan uitvoeren.*
1. De systeemeigenaar is verantwoordelijk voor het periodiek organiseren van hersteltesten per systeem. De frequentie waarmee de hersteltesten plaatsvinden is vastgelegd in stap 2.2B.
2. Let op dat bij het herstellen van data met behulp van in het verleden gemaakte back-ups de bewaartermijnen worden gehanteerd.

## Monitoren van back-ups

***Toelichting***

* *Beschrijf hoe afwijkingen op de toepassing van maatregelen 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 2.2B. Automatische back-ups worden beschikbaar gesteld zodat de systeemeigenaar afwijkingen kan identificeren.
2. De IBP’er voert <bepaalde frequentie> een tweedelijnscontrole uit op de toepassing van de maatregelen zoals vastgelegd in stap 2.2B en op de uitvoering van de hersteltesten uit stap 2.4A. 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 back-up- en herstelproces.

|  |  |
| --- | --- |
| **Rol**  | **Verantwoordelijkheden** |
| **Eerste lijn** |
| Bestuur, directie, schoolleiding | * <Vul aan met verantwoordelijkheden>.
 |
| Systeemeigenaar | * Vastleggen van back-upmaatregelen en hersteltesten in het CMDB.
* Controle op de implementatie en toepassing van de maatregelen.
* <Vul aan met verantwoordelijkheden>.
 |
| IT-medewerkers | * Implementeren back-upmaatregelen en uitvoeren hersteltesten in samenwerking met de systeemeigenaar.
* <Vul aan met verantwoordelijkheden>.
 |
| **Tweede lijn** |
| Proceseigenaar | * Opstellen en beheren van de back-up- en herstelprocesbeschrijving.
* <Vul aan met verantwoordelijkheden>.
 |
| IBP’er, CISO, security officer, privacy officer | * Periodieke controle op de geïmplementeerde back-upmaatregelen en hersteltesten.
* <Vul aan met verantwoordelijkheden>.
 |
| **Derde lijn** |
| Interne audit | * Bepaal of deze rol een functie heeft binnen dit proces.
* <Zo ja, vul aan met verantwoordelijkheden>.
 |