Template Incidentmanagementbeleid

Versienummer: 1.0

Januari 2024

Dit template Incidentmanagementbeleid is zorgvuldig 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 Incidentmanagementbeleid is opgesteld door Kennisnet en verschijnt onder de licentie Creative Commons Naamsvermelding 4.0 Nederland.

<https://creativecommons.org/licenses/by/4.0/legalcode.nl>

Bij het samenstellen van dit template is gebruik gemaakt van de volgende bron:

Handreiking Incident- en response management, Vereniging van Nederlandse Gemeenten/ Informatiebeveiligingsdienst voor gemeenten, licentie onder: CC BY-NC-SA 4.0.

Gebruikswijzer template Incidentmanagementbeleid

**Verwijder voor eigen gebruik van dit document deze en de voorgaande pagina.**

Deze gebruikswijzer is bedoeld als toelichting op het gebruik van dit template voor incidentmanagementbeleid (en niet als leeswijzer voor het beleid zelf). Het template helpt slechts als richtlijn voor de IBP’ers om te komen tot een specifiek incidentmanagementbeleid voor het eigen schoolbestuur. Met de zoek- en vervang functie kun je bijvoorbeeld wel snel de naam van het schoolbestuur invullen, maar daarmee is het document nog niet geschikt om aan een bestuur voor te leggen. Vaak zal IBP bovenschools geregeld worden. <naam schoolbestuur> kun je dan vervangen worden door de naam van de overkoepelende instelling.

De invulling van het incidentmanagementbeleid kan per schoolbestuur op onderdelen verschillen. Van invloed kunnen zijn:

* Grootte van het schoolbestuur (bijvoorbeeld niet voldoende personen om alle taken en rollen zuiver te scheiden).
* De politieke werkelijkheid binnen een schoolbestuur (een organisatieverandering is niet altijd wenselijk, of niet op dit moment; of er is een specifieke mandatenregeling die bepaalde verantwoordelijkheden anders belegt).
* Volwassenheid van IBP in het schoolbestuur (het beleid is bijvoorbeeld te veelomvattend als onderliggende taken, rollen en functies nog niet zijn ingevuld en niet snel kunnen worden ingevuld).
* Een schoolbestuur heeft meer of minder onderliggende documenten beschikbaar om aan te refereren.
* Vormgevingseisen.

Het schoolbestuur kan afhankelijk van bovenstaande situaties kiezen om:

* Elementen weg te laten (als er bijvoorbeeld geen procesmanager is, of geen CSIRT).
* Elementen naar een bijlage te verplaatsen of enkel te refereren aan een onderliggend document, of juist in plaats van een bijlage tekst in het hoofddocument op te nemen.
* Elementen verder uit te schrijven omdat er geen onderliggende documenten zijn.

Specifiek maken van dit document

|  |  |
| --- | --- |
| <tekst> | Vervang dit door tekst die passend is bij de eigen situatie, bijvoorbeeld <naam schoolbestuur> wordt ‘Schoolbestuur X’. |
|  |  |

# Incidentmanagementbeleid

## 1. Documentgeschiedenis

### 1.1 Revisies

|  |  |  |  |
| --- | --- | --- | --- |
| Versie | Datum | Auteur | Review |
| **0.1** | 1 jan 2024 | <Voornaam Achternaam> | Eerste concept uitgewerkt |
|  |  |  |  |
|  |  |  |  |

### 1.2 Goedkeuring

Vastgesteld door <naam schoolbestuur>, hierna te noemen “de school”

|  |  |  |  |
| --- | --- | --- | --- |
| Naam | Functie | Versie | Datum |
| <het schoolbestuur is eindverantwoordelijk en hier moet de hoogst verantwoordelijke in de instelling komen te staan> | <het schoolbestuur is eindverantwoordelijk en hier moet de hoogst verantwoordelijke in de instelling komen te staan> |  |  |

### 1.3 Document classificatie

|  |  |
| --- | --- |
| Classificatie | Beschrijving |
| **Openbaar** | Dit document mag zonder beperkingen worden gedeeld |
| **Vertrouwelijk** | Mag worden gedeeld met medewerkers van <naam schoolbestuur> (en eventueel organisaties X,Y,Z) |
| **Geheim** | Dit document is exclusief bestemd voor de volgende personen: (bijv. leden MT) |

Inhoud

[Incidentmanagementbeleid 2](#_Toc438885302)

[1. Documentgeschiedenis 3](#_Toc604095650)

[1.1 Revisies 3](#_Toc1795384552)

[1.2 Goedkeuring 3](#_Toc180768240)

[1.3 Document classificatie 3](#_Toc1169846977)

[2. Inleiding 4](#_Toc334535128)

[3. Uitgangspunten 5](#_Toc117093920)

## 2. Inleiding

Het incidentmanagementbeleid geeft richting aan de wijze waarop het bestuur van de school wenst om te gaan met incidenten en (cyber)beveiligingsincidenten.

Een incident is een onverwachte gebeurtenis in de ict-omgeving die de continuïteit van de bedrijfsvoering negatief kan beïnvloeden. Als een incident de beschikbaarheid, vertrouwelijkheid of integriteit van informatie verstoort, spreken we van een inbreuk op de informatiebeveiliging of een (cyber)beveiligingsincident.

## 3. Uitgangspunten

De volgende uitgangspunten worden gehanteerd:

* De incidenten worden afgehandeld volgens het door de school formeel vastgestelde incidentmanagementproces om doeltreffend en ordelijk te reageren op incidenten. Dit proces is bekend bij alle betrokkenen. In dit proces zijn de rollen en verantwoordelijkheden vastgesteld.
* Incidentmanagement gaat over het detecteren, vastleggen en afhandelen van incidenten. Belangrijk hierbij is dat medewerkers, docenten, leerlingen en derden een incident of inbreuk op de informatiebeveiliging herkennen en dit ook melden.
* Iedere medewerker, docent, leerling en derde is verantwoordelijk voor het signaleren en melden van incidenten en inbreuken op de informatiebeveiliging, inclusief datalekken. Incidenten en inbreuken dienen direct gemeld te worden.
* Om incidenten te melden zijn er binnen de school meldpunten. De incidenten worden vastgelegd in een incidentregister en (cyber)beveiligingsincidenten in het register beveiligingsincidenten en datalekken. De school heeft de route naar deze meldpunten duidelijk gecommuniceerd naar alle betrokkenen (medewerkers, docenten, leerlingen en derden).
* Het bestuur van de school wil leren van incidenten. Incidenten worden daarom geëvalueerd, zodat de procedures kunnen worden bijgesteld en beheersmaatregelen kunnen worden verbeterd.
* Incidenten met (cyber)beveiliging zijn herkenbaar vastgelegd.
* (Cyber)beveiligingsincidenten kennen mogelijk een vervolgprocedure. Het vast te leggen bewijsmateriaal voor juridisch en forensisch onderzoek wordt verzameld in overeenstemming met de voorschriften.
	+ [Hoe te handelen in geval van een incident | Nationaal Cyber Security Centrum (ncsc.nl)](https://www.ncsc.nl/onderwerpen/oekraine-hoe-te-handelen-in-geval-van-een-incident),
	+ [Bewaartermijnen - Aanpak informatiebeveiliging en privacy in het onderwijs (kennisnet.nl)](https://aanpakibp.kennisnet.nl/bewaartermijnen/)
* Periodiek rapporteert <naam, rol> aan <naam, rol> over de opgetreden incidenten en (cyber)beveiligingsincidenten en de impact op de bedrijfsvoering en onderwijs.