Template Incidentmanagementproces

Versienummer: 1.0

Januari 2024

Dit template Incidentmanagementproces 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 Incidentmanagementproces 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 Incidentmanagementproces 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 Incidentmanagementproces

**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 het incidentmanagementproces (en niet als leeswijzer voor het proces zelf). Het template helpt slechts als richtlijn voor IBP’ers om te komen tot een specifiek incidentmanagementproces 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 incidentmanagementproces 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 vooralsnog 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’. |
|  |  |

**Normen- en toetsingskader**

Deze template dient ter uitwerking en ondersteuning van norm 6.1 tot en met 6.3 van het Normenkader IBP voor het funderend onderwijs. De template voldoet aan de minimale eisen van het gestelde toetsingskader en is basis voor de voorbeeldmaatregelen.

Toetsingskader:

* Het incidentmanagementbeleid is formeel gedocumenteerd en gecommuniceerd.
* Rollen en verantwoordelijkheden van de organisatie en de leveranciers zijn duidelijk gedefinieerd.
* Aspecten van juridisch en forensisch onderzoek zijn vastgesteld en toegewezen.
* Het registreren van, de communicatie over en de toewijzing en analyse van incidenten zijn formeel belegd in de organisatie.
* Incidenten worden gecategoriseerd en geprioriteerd op basis van impact.
* (Cyber)beveiligingsincidenten worden voorkomen of gedetecteerd en er is een proces om deze tijdig en effectief aan te pakken.
* Informatie wordt proactief en formeel gedeeld met personeel.
* Er wordt gemonitord of incidenten tijdig worden opgelost.
* Er wordt beperkt gerapporteerd aan het management over incident- en oplossingsanalyses.
* Het formeel vastgelegde beleid voor incidentmanagement bevat een escalatieprocedure.
* Er zijn escalatiecriteria bepaald.
* De escalatieprocedure is gebaseerd op serviceniveaus voor incidenten die niet meteen opgelost kunnen worden.
* Categoriseren en prioriteren gebeurt op basis van impactanalyse, de bepaalde criteria en serviceniveaus.
* De responsteams krijgen de benodigde training.
* De verantwoordelijkheid voor het oplossen van een incident is toegewezen.
* Naast de gebruikelijke incidentmanagementprocedures zijn er plannen voor preventie, risicobeperking, voorbereiding, tijdige reactie en herstel van (cyber)beveiligingsincidenten.

**Doelgroep**

De doelgroep van dit document zijn de it-incidentprocesmanagers en de IBP-verantwoordelijken. Deze zorgen ervoor dat schoolbestuurders en andere betrokkenen hun verantwoordelijkheden kennen en daarnaar kunnen handelen. Ook coördineren ze de uitvoering van de werkzaamheden.

**Hoe te gebruiken**

De vastgestelde documenten zijn levende documenten en zullen jaarlijks geanalyseerd en geëvalueerd moeten worden. Ook wordt bij de evaluatie van elke grote verstoring/incident de werking van het incidentmanagementproces geëvalueerd. Wijzigingen van het proces dienen formeel bekrachtigt te worden door het schoolbestuur.

# Incidentmanagementproces

## 

## 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 evt. organisaties X,Y,Z) |
| **Geheim** | Dit document is exclusief bestemd voor de volgende personen: (bijv. leden MT) |

## Inhoudsopgave

[Incidentmanagementproces 3](#_Toc135997018)

[1. Documentgeschiedenis 4](#_Toc1031178879)

[1.1 Revisies 4](#_Toc1565912841)

[1.2 Goedkeuring 4](#_Toc1187848318)

[1.3 Document classificatie 4](#_Toc1348161854)

[Inhoudsopgave 5](#_Toc1367991462)

[2. Doel en definitie 5](#_Toc1135644167)

[3. Procesflow incidentmanagement 6](#_Toc1963378057)

[4. Rollen en verantwoordelijkheden 8](#_Toc2010715167)

[5. Beschrijving processtappen 10](#_Toc707274813)

[5.1 Registratie 11](#_Toc377890589)

[5.2 Classificatie 11](#_Toc789398153)

[5.3 Prioritering 12](#_Toc842803933)

[5.4 Toewijzing 13](#_Toc1820065618)

[5.5 Diagnose en onderzoek 13](#_Toc1914215722)

[5.6 Oplossing 14](#_Toc1337137404)

[5.7 Afsluiting 14](#_Toc673801901)

[5.8 Evaluatie en analyse 14](#_Toc1749304433)

[6. Communicatie 14](#_Toc59888392)

[7. Procesflow (cyber)beveiligingsincident 15](#_Toc1490141313)

[8. Aanvullende processtappen (cyber)beveiligingsincident 18](#_Toc994744982)

[Melding van een (cyber)beveiligingsincident 18](#_Toc1914196252)

[Toewijzen en escaleren van een (cyber)beveiligingsincident 18](#_Toc1326847436)

[Acties IBP-verantwoordelijke/FG 19](#_Toc396396740)

[Alarmeringsprocedure 19](#_Toc1083610077)

[9. Rapportage 19](#_Toc1580579499)

[Bijlage 1: (Cyber)beveiligingsincidenten en meldingsniveau matrix (aanpassen naar behoefte van de onderwijsinstelling) 20](#_Toc1001563026)

## 2. Doel en definitie

Het doel van incidentmanagement is om verstoringen en incidenten in de ict-omgeving effectief te identificeren, registreren, prioriteren, oplossen en beheren. Incidenten zijn onverwachte gebeurtenissen of problemen die de normale werking van de ict-omgeving verstoren en die moeten worden opgelost om de continuïteit van het onderwijs en ondersteunende werkprocessen te borgen.

Als door een incident de *beschikbaarheid*, *vertrouwelijkheid* of *integriteit* van informatie wordt verstoord, spreken we van een (cyber)beveiligingsincident. Voor deze incidenten kan, afhankelijk van de aard en ernst van het incident, een aanvullende procedure gelden. Bij de inrichting van incidentmanagement is het van groot belang om (cyber)beveiligingsincidenten snel te herkennen, vast te leggen en af te handelen.

Incidentmanagement draagt niet alleen bij aan een goede afhandeling van incidenten, maar ook aan het leren ervan om incidenten in de toekomst te voorkomen.

## 3. Procesflow incidentmanagement

Gebruikers / Docenten / Leerlingen

Incident manager

Meldpunt / Servicedesk

Behandelaar / Leverancier

1 Registratie

2 Classificatie

Service-request?

Afhandelen Service request

3 Prioritering

Calami-teit?

Crisis manage-ment

Informatie-beveiliging?

4 Toewijzing

5 Diagnose en onderzoek

6 Oplossing

Melder tevreden?

7 Afsluiting

E-mail

Telefonische melding

Mondelinge melding

ja

ja

ja

ja

nee

nee

nee

nee

8 Evaluatie en analyse

Problem management

(cyber) beveiligings incident

## 4. Rollen en verantwoordelijkheden

In onderstaand schema zijn de rollen en verantwoordelijken vastgelegd voor het uitvoeren van het incidentmanagement. Indien van toepassing worden hier de naam toegevoegd van de persoon of afdeling en de contactgegevens van degenen die binnen de school voor de rol zijn aangewezen.

|  |  |  |
| --- | --- | --- |
| Rol | Naam | Contact |
| **Gebruikers/docenten/leerlingen**   * Melden van incidenten * Aanleveren benodigde informatie * Accepteren van de oplossing |  |  |
| **Meldpunt/servicedesk**   * Registreren, classificeren en toewijzen van incidenten * Waar mogelijk oplossen van incidenten * Escaleren van incidenten * Informeren van de melders van incidenten | <Naam>  Bij afwezigheid:  <Naam 2> | Telefoon vast: <nummer>  Mobiel: <06-nummer>  Email: <e-mailadres>  Telefoon vast: <nummer>  Mobiel: <06-nummer>  Email: <e-mailadres> |
| **Incidentmanager**   * Beheer van het incidentproces * Coördinatie van de reactie op incidenten * Beoordelen toegekende prioriteit, waar nodig opstarten crisismanagement * Bewaken van de voortgang van incidentoplossing * Escalatie bij overschrijding oplostijden, wijziging van impact, urgentie en prioriteit * Communiceren met belanghebbenden, docenten, leerlingen, etc. over de status van incidenten, geschatte oplostijden en eventuele noodzakelijke acties * Maken van incidentrapportage en -analyse | <Naam>  Bij afwezigheid:  <Naam 2> | Telefoon vast: <nummer>  Mobiel: <06-nummer>  Email: <e-mailadres>  Telefoon vast: <nummer>  Mobiel: <06-nummer>  Email: <e-mailadres> |
| **Behandelaar (aansturen Leverancier)**   * Onderzoeken, diagnosticeren en oplossen van incidenten * Oorzaak achterhalen en herstelmaatregelen treffen * Werken volgens de prioriteiten en richtlijnen die zijn vastgesteld door de incidentmanager * Voortgang incident bewaken * Bijhouden logging van uitgevoerde activiteiten en oplossing | <Naam>  Bij afwezigheid:  <Naam 2> | Telefoon vast: <nummer>  Mobiel: <06-nummer>  Email: <e-mailadres>  Telefoon vast: <nummer>  Mobiel: <06-nummer>  Email: <e-mailadres> |
| **Behandelaar (leverancier 1, internet)**   * Verantwoordelijkheden en afspraken leverancier 1 | <Naam>  Bij afwezigheid:  <Naam2> | Telefoon vast: <nummer>  Mobiel: <06-nummer>  Email: <e-mailadres>  Telefoon vast: <nummer>  Mobiel: <06-nummer>  Email: <e-mailadres> |
| **Behandelaar (leverancier 2, etc.)**   * Verantwoordelijkheden en afspraken leverancier 2 | <Naam>  Bij afwezigheid:  <Naam2> | Telefoon vast: <nummer>  Mobiel: <06-nummer>  Email: <e-mailadres>  Telefoon vast: <nummer>  Mobiel: <06-nummer>  Email: <e-mailadres> |
| **IBP-verantwoordelijke/FG**   * Beoordelen incident en escaleren als (cyber)beveiligingsincident * Beoordelen prioriteit op grond van risicoanalyse, waar nodig opstarten crisismanagement * Coördineren afhandeling van beveiligingsincidenten * Beoordelen en afhandelen privacyaspecten zoals melding bij Autoriteit Persoonsgegevens, in afstemming met bevoegd gezag. | <Naam>  Bij afwezigheid:  <Naam2> | Telefoon vast: <nummer>  Mobiel: <06-nummer>  Email: <e-mailadres>  Telefoon vast: <nummer>  Mobiel: <06-nummer>  Email: <e-mailadres> |
| **<Nadere invulling door school>**  <Taak/verantwoordelijkheid> | <Naam>  Bij afwezigheid:  <Naam2> | Telefoon vast: <nummer>  Mobiel: <06-nummer>  Email: <e-mailadres>  Telefoon vast: <nummer>  Mobiel: <06-nummer>  Email: <e-mailadres> |
| **<Nadere invulling door school>**  <Taak/verantwoordelijkheid> | <Naam>  Bij afwezigheid:  <Naam2> | Telefoon vast: <nummer>  Mobiel: <06-nummer>  Email: <e-mailadres>  Telefoon vast: <nummer>  Mobiel: <06-nummer>  Email: <e-mailadres> |

## 5. Beschrijving processtappen

### 5.1 Registratie

Indienen en registreren van een melding vindt plaats middels:

* E-mail naar: <e-mailadres servicedesk of meldpunt incidenten>
* Telefonische of mondelinge melding naar <naam> <telefoonnummer>

Benodigde informatie:

* Contactgegevens melder
* Beschrijving incident
* Datum/tijdstip

Controleer de melding op volledigheid en verzamel informatie over het incident (symptomen, screenshots, nadere uitleg). Als de melding niet volledig is, maak deze dan volledig in overleg met de aanmelder.

Registreer de melding in de servicedesk-applicatie (bijvoorbeeld TopDesk) of het register (Beveiligings)incidenten en datalekken (te vinden op de Aanpak IBP). De volgende informatie wordt vastgelegd:

* Een unieke identificatie/nummer
* Datum en tijd van de melding
* Datum en tijd waarop het incident heeft plaatsgevonden
* Wie de melding heeft gedaan
* Wie getroffen zijn door het incident
* Beschrijving van het incident
* Locatie van het incident
* Impact, urgentie en prioriteit van het incident
* Categorie
* De oplosgroep/medewerker die het incident behandelt
* Status, deze is initieel ‘Gemeld’
* Logging van uitgevoerde activiteiten om het incident te verhelpen
* Datum en tijd van de oplossing

Stuur de aanmelder een bericht met het meldingsnummer.

Zoek of er een openstaande melding is van hetzelfde incident. Zo ja, vermeld dit in het register, maak een verwijzing en sluit de melding.

Bepaal of er een bekende oplossing of workaround beschikbaar is. Zo ja, breng de melder op de hoogte, pas het incidentenregister aan en sluit de melding.

Zoek in het changeregister of er een change is geweest die mogelijk een relatie heeft met het incident. Zo ja, leg dit dan met de identificatie van de change vast in het incidentenregister en breng de betreffende changemanager op de hoogte.

### 5.2 Classificatie

Zijn de ict-componenten (assets) vastgelegd in een register? Zoek dan daar het Configuration Item (CI) dat in storing is en het incident veroorzaakt. Neem dan de classificatie en de behandelaar over uit dit register.

Is er geen register aanwezig? Leg dan een eenduidige beschrijving van de verstoorde componenten vast in het incidentenregister. Classificeer het incident met behulp van onderstaand schema. Het is mogelijk voor één incident meerdere classificaties toe te kennen.

Een mogelijke nadere onderverdeling is te vinden in [FORA: Funderend Onderwijs Referentie Architectuur](https://www.kennisnet.nl/diensten/fora-funderend-onderwijs-referentie-architectuur/)

|  |  |  |
| --- | --- | --- |
| Classificatie | Behandelaar | Criteria/voorbeelden |
| Hardware | <Naam medewerker/afdeling/ externe leverancier>  <Contactgegevens> | <Netwerkstoring  Laptop/desktop defect  et cetera> |
| Software | <Naam medewerker/afdeling/ externe leverancier>  <Contactgegevens> | <Kantoorapplicaties niet beschikbaar  Foutieve werking applicatie  et cetera> |
| Netwerk LAN | <Naam medewerker/afdeling/ externe leverancier>  <Contactgegevens> | <Netwerkkabel defect  DNS-fouten, geen wifi  et cetera> |
| Netwerk WAN | <Naam medewerker/afdeling/ externe leverancier>  <Contactgegevens> | <Geen internetverbinding  Traag internet  et cetera> |
| <Verder aanvullen naar behoefte van de school> |  |  |

**Datalek en/of vermoeden van een (cyber)beveiligingsincident**

Als door een incident de *beschikbaarheid*, *vertrouwelijkheid* of *integriteit* van informatie wordt verstoord, spreken we van een (cyber)beveiligingsincident.

Is er een vermoeden dat de melding een datalek en/of beveiligingsincident betreft? Markeer de melding dan als informatiebeveiligingsincident.

**Beschikbaarheid**: verlies van data, Informatiesysteem niet beschikbaar, etc.

**Integriteit**: malwareaanval, informatie onbedoeld gewijzigd, etc.

**Vertrouwelijkheid**: ongeautoriseerde toegang, informatie naar anderen verspreid, etc.

Zie ook bijlage 1 voor een opsomming van mogelijke (cyber)beveiligingsincidenten.

### 5.3 Prioritering

Bepaal de impact en de urgentie van het incident volgens de criteria in onderstaand schema. Dit bepaalt de prioriteit.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Prioriteit** | | | **Urgentie** | | |
| **Hoog** | **Midden** | **Laag** |
| Kan niet werken | Kan deels werken | Kan werken |
| **Impact** | **Hoog** | Hele organisatie/ school/primair onderwijsproces | 1 Calamiteit | 2 Hoog | 3 Midden |
| **Midden** | Team/afdeling | 2 Hoog | 3 Midden | 4 Laag |
| **Laag** | Eén of een beperkt aantal eindgebruikers | 3 Midden | 4 Laag | 4 Laag |

Escaleer incidenten met prioriteit ‘calamiteit’ en ‘hoog’ onmiddellijk naar de incidentmanager.

**Maximale doorlooptijden**

* Calamiteit: z.s.m., te bepalen door crisismanagementteam
* Hoog: 8 uur
* Middel: 3 werkdagen
* Laag: 5 werkdagen

De doorlooptijden van openstaande incidenten worden bewaakt door de incidentmanager en bij overschrijding geëscaleerd bij behandelaren/leveranciers of het schoolbestuur. Overschrijding van de doorlooptijden kan leiden tot aanpassing van de prioriteit en daarmee tot escalatie naar het crisismanagementteam.

### 5.4 Toewijzing

Bepaal behandelaar of externe leverancier met behulp van de classificatie

Informeer de behandelaar of externe leverancier over het incident

Bij een (cyber)beveiligingsincident:

* Informeer de incidentmanager en de IBP-verantwoordelijke/FG
* Leg (cyber)beveiligingsincident vast in applicatie/register (cyber)beveiligingsincidenten

Werk in het incidentenregister de status bij naar ‘Onderhanden’

### 5.5 Diagnose en onderzoek

Leg alle stappen vast in de logging van het incidentregister

Controleer of het incident is toegewezen aan de juiste behandelaar. Zo nee, informeer meldpunt/servicedesk.

Verzamel aanvullende informatie. Als er aanvullende informatie nodig is, neem dan contact op met de melder. Als deze niet direct te bereiken is stuur je een mail met de vraag om aanvullende informatie. Verander de status in het incidentenregister naar ‘Wacht op antwoord’.

Als een oplossing mogelijk is ga dan verder met stap 5.6 Oplossing.

### 5.6 Oplossing

Neem de oorzaak van het incident weg of bepaal een work-around.

Werk het incidentenregister bij met de benodigde informatie.

Overleg, waar nodig via de servicedesk, met de melder of de oplossing voldoet.

Als de oplossing een change nodig heeft, dien je een ‘request for change’ (RFC) (wijzigingsverzoek) in volgens het proces changemanagement (verwijzing).

Verander de status in het incidentenregister naar ‘Opgelost’.

### 5.7 Afsluiting

Controleer bij de melder of het probleem is opgelost. Zo ja, werk dan het incidentenregister bij met status en datum/tijd.

Geeft de melder aan dat het incident nog niet is opgelost? Informeer dan de behandelaar/externe leverancier.

Verander de status in het incidentenregister naar ‘Afgesloten’.

### 5.8 Evaluatie en analyse

Vraag aan de melder feedback over de oplossing en het gevolgde incidentproces om mogelijke verbeteringen te identificeren.

Onderzoek of er andere, gelijksoortige, incidenten zijn (geweest) waarvan de eenduidige oorzaak bekend is. Informeer waar nodig de problemmanager. Het proces probleemmanagement kan mogelijk deze eenduidige oorzaak wegnemen.

Evalueer voor incidenten met prioriteit hoog en calamiteit met de betrokkenen de werking van het incidentmanagementproces. Doe waar nodig verbetervoorstellen aan de incidentmanager.

## 6. Communicatie

In onderstaand schema is de communicatie tijdens de uitvoering van het incidentmanagementproces vastgelegd.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Prioriteit/  Gebeurtenis | Omschrijving Communicatie | Verantwoordelijk | Medium | Frequentie | Ontvanger |
| Melding Incident | Bevestiging melding | <rol> | <bijv. Mail> | Eénmalig | Melder |
| Escalatie crisis |  | <rol> | <bijv. Chat / telefoon> | Eénmalig | Bestuur  Incidentmanager  FG  IBP verantwoordelijke |
| Laag | Voortgang | <rol> | <bijv. Mail> | Wekelijks | Melder |
| Midden | Voortgang | <rol> | <bijv. Mail> | Dagelijks | Melder |
| Hoog | Voortgang | <rol> | <bijv. Mail> | 2 keer per dag | Melder |
| Calamiteit |  | <rol> |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## 7. Procesflow (cyber)beveiligingsincident

Gebruikers / Docenten / Leerlingen / incidentmanager

Meldpunt / Servicedesk

Incidentmanager / IBP verantwoordelijke / FG / schoolbestuur

Behandelaar / Leverancier

E-mail

Telefonische melding

Mondelinge melding

0.Detectie

1.Initiatie

2.Analyse

3.Schade indamming en beoordeling van de blootstelling

4. Remediatie en herstel

5.Kennisgeving

Datalek?

Incident management

Melding aan AP

Melding Potentieel Datalek

ja

nee

## 8. Aanvullende processtappen (cyber)beveiligingsincident

### 

#### Melding van een (cyber)beveiligingsincident

Medewerkers, docenten, leerlingen en andere betrokkenen zoals leveranciers dienen alert te zijn op bedreigingen rond informatiebeveiliging en melden deze bij de servicedesk of meldpunt voor ict-incidenten.

#### Toewijzen en escaleren van een (cyber)beveiligingsincident

Bijlage 1 bevat een lijst (twee tabellen) met mogelijke incidenten (cyber)beveiligingsincidenten. Deze lijst is niet uitputtend en kan dit ook niet zijn: er zullen zich steeds nieuwe soorten beveiligingsincidenten voordoen. De lijst ondersteunt de incidentmanager/servicedesk bij het herkennen van een (cyber)beveiligingsincident en bij het inschatten van de impact. Bij twijfel vindt overleg plaats met de IBP-verantwoordelijke/FG.

In veel gevallen zal de IBP-verantwoordelijke/FG niet als primaire behandelaar optreden. Het technisch verhelpen van een dergelijk incident gebeurt niet door de IBP-verantwoordelijke/FG, maar door een specialist.

In de servicedeskapplicatie of het register (beveiligings)incidenten en datalekken (beschikbaar op de Aanpak IBP) wordt een extra (cyber)beveiligingsincident aangemaakt. Leg het volgende vast:

* Identificatie
* Datum tijd van het incident
* Datum tijd van de melding
* Wie is de melder?
* Is de FG ingeschakeld?
* Wat is er met de informatie gebeurd?
* Wie is/zijn getroffen?
* Welke informatie betreft het?
* Aantal betrokkenen
* Korte toelichting
* (Mogelijke) gevolgen voor de betrokkene(n)
* Getroffen maatregelen om gevolgen te beperken
* Datalek ja/nee
* AP melden ja/nee?
* AP datum: <datum>
* AP tijdstip: <tijdstip>
* Melding binnen 72 uur, ja/nee?
* Betrokkene(n) melden j/n?
* Melding Datum tijdstip, wijze van benadering
* Datum klaar

De IBP-verantwoordelijke/FG kan op twee manieren worden ingeschakeld:

* De IBP-verantwoordelijke/FG moet een (cyber)beveiligingsincident met hoge prioriteit direct oplossen, dan wel coördineren of adviseren. In dit geval neemt de helpdesk direct telefonisch contact op met de IBP-verantwoordelijke/FG (of vervanger).
* De IBP-verantwoordelijke/FG moet op de hoogte worden gebracht dat een incident heeft plaatsgevonden. De IBP-verantwoordelijke/FG raadpleegt daarvoor regelmatig het incidentenregister (ongeveer 1 keer per maand).

#### Acties IBP-verantwoordelijke/FG

De IBP-verantwoordelijke/FG neemt waar nodig direct maatregelen om relevant bewijsmateriaal en andere gegevens veilig te stellen.

De IBP-verantwoordelijke/FG adviseert hoeveel tijd en middelen nodig zijn voor afhandeling van het beveiligingsincident. Aan de hand hiervan en de impact van het incident bepaalt het schoolbestuur in overleg met de IBP-verantwoordelijke/FG de teamsamenstelling.

De IBP-verantwoordelijke/FG coördineert de afhandeling en vastlegging van de uitgevoerde activiteiten met behulp van de template (cyber)beveiligingsincident-stappenplan en -logboek (te vinden op de Aanpak IBP).

#### Alarmeringsprocedure

Als de IBP-verantwoordelijke/FG inschat dat de ernst van het incident dusdanig is óf dat acties nodig zijn die de handelingsbevoegdheid van de IBP-verantwoordelijke/FG te boven gaan, wordt samen met de incidentmanager het proces crisismanagement geactiveerd. Lees daar meer over via [(Cybersecurity)crisis: hoe bereid je je voor?](https://www.kennisnet.nl/artikel/21437/cybersecuritycrisis-hoe-bereid-je-je-voor-oefen-met-de-bob-methode-2/)

## 9. Rapportage

Met als bron de administratie van incidenten/(cyber)beveiligingsincidenten of het register wordt <wekelijks / maandelijks> gerapporteerd.

Er wordt gerapporteerd over de volgende Key Performance Indicators (KPI's).

|  |  |  |
| --- | --- | --- |
|  | **KPI** | **OMSCHRIJVING** |
|  | Aantal nieuwe incidenten gemeld | Totaal aantal nieuwe incidenten gemeld in de afgelopen periode. |
|  | Incidenten opgelost, door de servicedesk, door behandelaar, door leverancier | Totaal aantal incidenten die in de afgelopen periode zijn opgelost gespecificeerd naar oplosgroep. |
|  | Aantal nieuwe (cyber)beveiligingsincidenten gemeld | Totaal aantal incidenten die als (cyber)beveiligingsincident aangemerkt zijn. |
|  | Aantal (cyber)beveiligingsincidenten opgelost | Totaal aantal (cyber)beveiligingsincidenten die in de afgelopen periode zijn opgelost. |
|  | Aantal openstaande incidenten calamiteit/hoog/midden/laag | Totaal aantal nog niet opgeloste incidenten gespecificeerd naar prioriteit. |
|  | Korte evaluatie van incidenten met de prioriteit calamiteit of hoog. | Beschrijving van de oplossing, aanbevelingen en gevraagde beslissingen naar aanleiding van evaluatie. |
|  |  |  |

## Bijlage 1: (Cyber)beveiligingsincidenten en meldingsniveau matrix (aanpassen naar behoefte van de onderwijsinstelling)

| **GEBRUIKERSINCIDENTEN** | | **NIVEAU VAN MELDING \*)** | | |
| --- | --- | --- | --- | --- |
| **Incidenten categorie** | **Incident** | **Meldpunt / servicedesk** | **IBP-verantwoor- delijke/FG** | **Bestuur** |
| Onopzettelijk foutief handelen | Als gevolg van foutieve procedures | X |  |  |
|  | Als gevolg van foutgevoelige bediening | X |  |  |
|  | Onzorgvuldige omgang met password | X |  |  |
| Opzettelijk foutief handelen | Niet volgen van voorschriften | X | X | (X) |
|  | Fraude of diefstal | X | X | X |
|  | Ongeautoriseerde toegang door medewerker | X | X | X |
| Technisch falen van apparatuur | Storing in laptop, pc of randapparatuur | X |  |  |
| Technisch falen van apparatuur door externe invloeden | Wegvallen elektrische spanning | X | X |  |
| Menselijke omgang met apparatuur | Bedieningsfouten | X |  |  |
| Opzettelijke wijzigingen | X | X | (X) |
|  | Beschadiging of vernieling | X | X | X |
| Problemen met programmatuur | Fouten in programmatuur | X |  |  |
|  | Ongeautoriseerd gebruik | X | X |  |
|  | Wijziging door medewerker | X | X | X |
|  | Opzettelijk introduceren van een virus door medewerker | X | X | X |
|  | Inbrengen van virus door middel van niet-gescreende programmatuur | X | X | X |
|  | Illegaal kopiëren | X | X | X |
|  | Diefstal van programmatuur | X | X | X |
| Gegevens en gegevens­dragers | Zoekraken gegevensdragers | X | X | X |
|  | Diefstal van gegevensdragers | X | X | X |
|  | Beschadiging gegevensdragers | X |  |  |
|  | Onleesbaarheid van gegevensdragers | X |  |  |
|  | Fouten in gegevens door apparatuur | X |  |  |
|  | Fouten in gegevens door programmatuur | X |  |  |
|  | Opzettelijke invoer van foutieve gegevens | X | X | X |
|  | Onopzettelijke invoer van foutieve gegevens | X |  |  |
|  | Illegaal kopiëren van gegevens | X | X | X |
|  | Ongeoorloofd inzien van gegevens bijvoorbeeld bij invoer of printen | X | X | X |
|  | Onzorgvuldige vernietiging van gegevens | X | X | X |
| Omstandigheden op de werkplek | Uitval van elektriciteit | X |  |  |
| Wateroverlast door lekkage | X |  |  |
| (Faciliteiten) | Ongewenste trillingen | X |  |  |

| **BEHEER­INCIDENTEN** |  | **NIVEAU VAN MELDING \*)** | | |
| --- | --- | --- | --- | --- |
| **Incidenten categorie** | **Incident** | **Meldpunt / servicedesk** | **IBP verantwoor- delijke / FG** | **Bestuur** |
| Identificatie en bevoegdheden van gebruikers | Geen eenduidige gebruiker bij een gebruikersnaam geconstateerd | X | X |  |
|  | Ongeautoriseerde toegang door medewerker | X | X | X |
|  | Er komen gebruikers voor die niet meer bevoegd zijn (ex-medewerkers/docenten/ leerlingen) | X | X |  |
|  | Vraagtekens bij bevoegdheden van bepaalde gebruikers of beheerders | X | X |  |
| Onopzettelijk foutief handelen van gebruikers | Onzorgvuldige omgang met wachtwoorden door gebruikers | X | X |  |
| Opzettelijk foutief handelen van gebruikers | Kraken of omzeilen toegang door medewerkers/docenten/leerlingen of een buitenstaander | X | X | X |
|  | Fraude of diefstal | X | X | X |
| Technisch falen van apparatuur | Storing in apparatuur | X | (X) |  |
| Technisch falen van apparatuur door externe invloeden | Wegvallen elektrische spanning of spanningsschommelingen | X | X | X |
|  | Wateroverlast | X | X | X |
|  | Uitval netwerkverbinding door aanval met grote hoeveelheden data | X | X | X |
| Omgang met apparatuur door gebruikers of derden | Beschadiging apparatuur | X | X | X |
| Diefstal van apparatuur | X | X | X |
|  | Apparatuur blijkt niet geregistreerd | X |  |  |
|  | Geregistreerde apparatuur blijkt niet aanwezig | X | X |  |
| Onopzettelijk foutief handelen | Fouten in handleiding | X |  |  |
| Problemen met programmatuur | Fouten in programmatuur | X | (X) |  |
|  | Ongeautoriseerde wijzigingen in programmatuur | X | X |  |
|  | Introductie van virussen via programmatuur | X | X | X |
|  | (On)opzettelijk ongeautoriseerd gebruik | X | X |  |
|  | Gebruik van ongeautoriseerde programmatuur | X | X |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Gegevens en gegevensdragers | Ongeautoriseerde toegang tot gegevens | X | X | X |
|  | Zoekraken gegevensdragers | X | X | X |
|  | Diefstal van gegevensdragers | X | X | X |
|  | Beschadiging gegevensdragers | X |  |  |
|  | Onleesbaarheid van gegevensdragers | X |  |  |
|  | Fouten in gegevens door apparatuur | X |  |  |
|  | Fouten in gegevens door programmatuur | X |  |  |
|  | Opzettelijke invoer van foutieve gegevens | X | X | X |
|  | Onopzettelijke invoer van foutieve gegevens | X |  |  |
|  | Illegaal kopiëren van gegevens | X | X | X |
|  | Ongeoorloofd inzien van gegevens bijvoorbeeld bij invoer of printen | X | X | X |
|  | Onzorgvuldige vernietiging van gegevens | X | X | X |
| Facilitaire structuren en omgeving | Kortsluiting /stroomuitval | X | X | X |
| Wateroverlast door lekkage | X | X | X |
|  | Ongeoorloofde toegang tot computer­ruimte | X | X | X |
|  | Uitgifte sleutels aan ongeautoriseerde | X | X | X |
| Diensten van derden | Cruciale diensten worden (tijdelijk) niet of onvoldoende geleverd | X | X |  |
|  | Niet gescreend personeel |  | X | X |
|  | Schending vertrouwelijkheid | X | X | X |
|  | Misbruik van toevertrouwde middelen (gegevens, documentatie, en dergelijke) | X | X | X |
|  | Incidenten worden niet gemeld | X | X | X |
|  | Incidenten met informatie van de school | X | X | X |

\*) Niveau van Melding:

* Meldpunt/servicedesk: incidenten die door gebruiker, docenten, leerlingen en/of beheerder worden gemeld bij het meldpunt/de servicedesk.
* IBP-verantwoordelijke/FG: Incidenten die door meldpunt/servicedesk worden gemeld bij de IBP-verantwoordelijke/FG.
* Bestuur: Incidenten die door IBP-verantwoordelijke/FG worden gemeld bij het schoolbestuur.