



Publicatie op intranet: 18 mei 2022

# Procedure Incidentmeldingen

Deze procedure beschrijft de taken en verantwoordelijkheden van alle betrokkenen bij een incident:

- De proceseigenaar: is verantwoordelijk voor het oplossen van beveiligingsincidenten binnen de eigen processen.
- Alle medewerkers: zijn verplicht om (een vermoeden van) een beveiligingsincident of datalek binnen 24 uur te melden.
- De behandelaar: is verantwoordelijk voor de behandeling van de meldingen in zijn of haar werkvoorraad. De behandelaar voert de regie over de inzet van onderaannemers (leveranciers, functioneel beheerders, eindgebruikers, etc.).
- De leverancier: als leverancier van systemen en diensten, maar ook als onderaannemer bij de behandeling van incidenten.

## Begrippen

### Behandelaar

De behandelaar is degene die de melding op zijn of haar naam heeft staan. Dit is meestal de helpdeskmedewerker 2<sup>e</sup> lijn (systeembeheerder), functionaris gegevensbescherming (FG) of de functioneel beheerder.

### Helpdesk

De helpdesk is de ICT-klantenservice voor onze medewerkers. Je kunt bij de helpdesk terecht op werkdagen van 8:00 –17:00. De I&A medewerkers hebben hiervoor diensten als helpdeskmedewerker 1<sup>e</sup> lijn. Tijdens een dienst:

- Wordt het telefoonnummer xxx opgenomen;
- Wordt de e-mail box [xxx@lochem.nl](mailto:xxx@lochem.nl) leeg gehouden (door direct af te handelen of te registreren in TOPdesk);
- Worden mondelinge, telefonische en per e-mail binnengekomen meldingen in TOPdesk gezet (ook uit privé-mailbox);
- Worden binnenkomende TOPdesk-meldingen beoordeeld (STAP 3);
- Worden binnenkomende TOPdesk-meldingen verdeeld (STAP 3).

### Incident

Een **incident** is een verstoring: iets dat je al had, werkt niet meer, of werkt niet meer zoals bedoelt.

### Informatiebeveiligingsincident

Een **informatiebeveiligingsincident** (of beveiligingsincident) is een gebeurtenis waarbij de mogelijkheid bestaat dat de beschikbaarheid, de integriteit of de vertrouwelijkheid van informatie of informatiesystemen in gevaar is of kan komen. Dit komt overeen met de kruisjes in de kolom 'CISO' van bijlage 2.

### Wijziging

Een **wijziging** is een verandering in de omgeving, waarbij iets nieuws wordt gevraagd. Het gaat hier dus om iets dat je nog niet had. De aanvraag van een wijziging start deze procedure op.

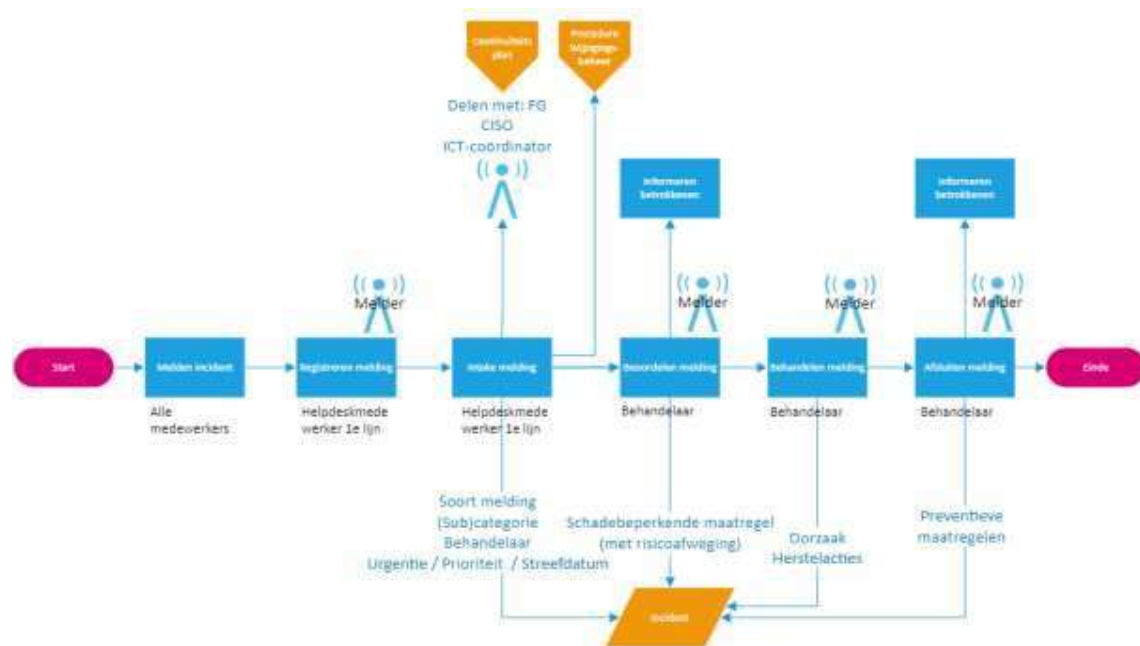


Publicatie op intranet: 18 mei 2022

# Procedure Incidentmeldingen

## Processtappen

### Procesmodel Incidentmeldingen (Visio)



## Aanleiding (detectie)

Een medewerker, detectiesysteem, leverancier, IBD, de pers of andere constateert een incident.

## Hulpmiddelen

- TOPdesk: Incidentregistratie:
  1. Soort, categorie en subcategorie van de melding
  2. Melding delen met ICT-coördinator, FG en CISO.
  3. Urgentie en prioriteit.
  4. Maatregelen en de risicoafweging.
  5. Behandeling van meldingen.
- TOPdesk: Contactpersonen leveranciers bij incidenten.
- [xxxx@lochem.nl](mailto:xxxx@lochem.nl): Gezamenlijke mailbox I&A. Op deze mailbox komen de meldingen van leveranciers, de informatiebeveiligingsdienst (IBD) en andere instanties binnen.
- xxx: Helpdesk telefoon
- Coordinated Vulnerability Disclosure (CVD): Een meldpunt en procedure voor (ethische) hackers om kwetsbaarheden te melden.

## STAP 1: Melden incident (initiatie)

Uitvoerder: Elke medewerker (dus ook de helpdeskmedewerker zelf)



Publicatie op intranet: 18 mei 2022

## Procedure Incidentmeldingen

- a. Op het moment dat je een incident vermoedt, meld je dit zo snel mogelijk, maar in elk geval binnen 24 uur bij de helpdesk (in volgorde van voorkeur):
  1. In TOPdesk
  2. In de mailbox van [servicedesk@lochem.nl](mailto:servicedesk@lochem.nl)
  3. Via de telefoon (als je niet kunt werken)
  4. Door een bezoekje

Bij meldingen in TOPdesk worden de stappen 2 en 3, waar mogelijk, automatisch doorlopen.

### STAP 2: Registreren melding in TOPdesk (initiatie)

Uitvoerder: Helpdeskmedewerker 1<sup>e</sup> lijn

- a. Beoordeel alle e-mails in de mailbox van [servicedesk@lochem.nl](mailto:servicedesk@lochem.nl).
- b. Beoordeel vragen via telefoon en bezoek.
- c. Registreer e-mails, telefoontjes en bezoekjes in TOPdesk als<sup>1</sup>:
  1. Er sprake is van een (mogelijk) incident.
  2. Als er sprake is van een (mogelijke) wijziging in een configuratie item.
  3. Als je de vraag / storing niet zelf kan beantwoorden / verhelpen.
  4. Als je de vraag / storing niet tijdens jouw dienst kan beantwoorden / verhelpen.
  5. Als je twijfelt.

### STAP 3: Intake van de melding (analyse)

Uitvoerder: Helpdeskmedewerker 1<sup>e</sup> lijn

- a. Bepaal het soort melding en de classificatie. In [Bijlage 1 Soort melding, categorie en subcategorie](#) staat wanneer je kiest voor welke soort en classificatie.
- b. Is er sprake van een **informatiebeveiligingsincident** (categorie), dan deel je de melding met de ICT-coördinator en de CISO als:
  1. De impact hoog is (gebruik hiervoor de voorbeelden uit Bijlage 3: Incident Impact bepaling)
  2. Er een (vermoede van) opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatie verwerkende systemen is.

Als je twijfelt deel je de melding ook met de betrokkenen. De ICT-coördinator en de CISO maken dan zelf de afweging.

**AFSPRAAK:** De ICT-coördinator en CISO bepalen in overleg of het Continuïteitscrisisteam (CCT) moet worden opgestart. Daarna wordt het continuïteitsplan gevolgd.

---

<sup>1</sup>TOPdesk zorgt voor registratie, maar ook voor communicatie richting eindgebruiker bij elke stap ontvangt de melder een notificatie.



Publicatie op intranet: 18 mei 2022

## Procedure Incidentmeldingen

- c. Is er sprake van een (vermoeden van) een **datalek** (subcategorie), dan zet je de melding op de groep Datalek. De FG en de CISO (als vervanger) zijn lid van deze groep en worden behandelaar van deze melding. Bij twijfel zet je de melding ook op de groep Datalek. Zij maken dan zelf de afweging.

**AFSPRAAK:** De FG, CISO en de proceseigenaar bepalen in overleg of er sprake is van een echt datalek, of de FG deze meldt bij de Autoriteit Persoonsgegevens (AP) en welke corrigerende maatregelen worden genomen. Het verslag wordt in de datalekmelding vastgelegd. Daarna zet de FG de melding door naar degene die de uitvoering van de maatregelen bewaakt.

- d. Bepaal de prioriteit: in het vakje Planning vul je impact en urgentie in. TOPdesk bepaalt zelf de prioriteit.
- e. Bepaal de streefdatum: TOPdesk stelt zelf een doorlooptijd voor. Deze kan je aanpassen.

**AFSPRAAK:** Beveiligingsmeldingen krijgen een urgentie (NCSC-classificatie kwetsbaarheidswaarschuwingen) mee. Als de kans op misbruik en de verwachte schade beide hoog zijn, worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd.

- f. Los de melding zelf direct op, als:
- De melding opgelost kan worden met een kennisitem.
  - Je kan het zelf én (later) op dezelfde dag oplossen. Maak hier een kennisitem van (als dat zin heeft)
  - Het een standaard wijzigingen (IDU = In dienst – Doorstroom - Uit dienst, rechten, ....), aanmaken en innemen gebruikersaccounts en gebruikersapparatuur.
  - Het gaat om werkplek ondersteuning en instructie.
  - Er geen (nieuwe) meldingen meer zijn voor stap 2 of 3.

Ga door naar STAP 6.

- g. Los je de melding niet op dezelfde dag of zelf op? Bepaal dan de behandelaarsgroep. Wijs hem eventueel toe aan een specifieke behandelaar. Of aan jezelf. Eventueel voorzien van een opmerking voor de volgende behandelaar (met 'onzichtbaar voor aanmelder' aangeklikt). Is de volgende behandelaar de helpdeskmedewerk 2<sup>e</sup> lijn, geef dan in de opmerking aan waarom je de melding niet zelf oppakt.

**AFSPRAAK:** Als de melder het informatiesysteem kan opstarten (de melder ziet minimaal een inlogschermb) dan is de melding voor de functioneel beheerder. Kan de melder het informatiesysteem niet opstarten, is de melding voor het team I&A (SSO is een uitzondering).

**AFSPRAAK:** Deze stap wordt afgerond binnen 1 werkdag nadat het incident is gemeld (STAP 1).



Publicatie op intranet: 18 mei 2022

# Procedure Incidentmeldingen

## STAP 4: Beoordelen van de melding (analyse, schadebeperking)

Uitvoerder: Behandelaar

- a. Controleer of er echt sprake is van een incident (vraag bepalen).
  - Wat is er gebeurd?
  - Hoe kon dit gebeuren?
  - Hoe lang is dit al aan de hand?
  - Om welke systemen en applicaties gaat het?
  - Welke persoonsgegevens zijn er geraakt?
  
- b. Onderzoek mogelijke gevolgschade.

Bijvoorbeeld of dit incident (op termijn) voor andere incidenten zorgt. Doe dit vooral in overleg met de melder.
  
- c. Beperk eventuele (vervolg) schade. Voorbeelden van maatregelen zijn:
  - Zorg voor een tussenoplossing (workaround).
  - Zet apparatuur niet uit die aanstaat.
  - Verbreek eventueel de netwerkverbinding.
  - Stel back-ups veilig.
  - Zet de automatische back-up uit.
  - Stel logfiles veilig.

Beschrijf de vraag (a.), eventuele vervolgschade (b.), maatregelen en de risicoafweging (c.) bij de melding.

**AFSPRAAK:** *Beveiligingsmeldingen krijgen een urgentie (NCSC-classificatie kwetsbaarheidswaarschuwingen) mee. Als de kans op misbruik en de verwachte schade beide hoog zijn neem je, zolang de kwetsbaarheid niet is verholpen, altijd mitigerende maatregelen op basis van een risicoafweging.*

- d. Bepaal wie getroffen is of wordt door dit incident. Hebben veel gebruikers last van het incident, dan informeer je alle betrokkenen:
  - Maak een nieuwsbericht op basis van het sjabloon. Of vraag de Webredactie een nieuwsbericht te plaatsen.
  - Stuur een link van het nieuwsbericht naar de functioneel beheerder en het afdelingshoofd.
  - De functioneel beheerders informeren hun eindgebruikers en de functioneel beheerder van een gekoppeld informatiesysteem. Een gekoppeld informatiesysteem is ook een eindgebruiker.
  - Alleen voor Team I&A:
    - i. Maak een nieuwsbericht in TOPdesk met een link naar het nieuwsbericht op Leo.
    - ii. Zet eventueel een bandje aan op **xxxx** over de string.



Publicatie op intranet: 18 mei 2022

## Procedure Incidentmeldingen

### STAP 5: Behandelen melding (oplossen, herstel)

Uitvoerder: Behandelaar

**AFSPRAAK:** Heb je een collega of leverancier nodig voor het behandelen van de melding? Betrek ze bij de behandeling. Jij blijft verantwoordelijk.

**AFSPRAAK:** Als je de melding overdraagt aan een collega, informeer je de melder altijd. Ga je er langer over doen, beoordeel dan zelf of je de melder hierover informeert. Dat is niet altijd nodig.

- a. Neem de oorzaak weg.
- b. Herstel naar de 'normale' situatie.
- c. Maak, indien nodig en mogelijk, een kennisitem. Begin een kennisitem met een kernwoord (dan sorteert het op onderwerp).
- d. Beschrijf de oorzaak en de herstelacties in de incidentregistratie. Eventueel in de vorm van een kennisitem.
- e. Zet, als dat nodig is, de melding door naar een volgende behandelaar. Eventueel voorzien van een opmerking voor de volgende behandelaar (met 'onzichtbaar voor aanmelder' aangeklikt).
- f. Als je in een eerder stadium een nieuwsbericht hebt gemaakt en de oplossing laat nog even op zich wachten:
  - Pas het nieuwsbericht op Leo en in TOPdesk aan met extra informatie.
  - Stuur een link van het nieuwsbericht naar de functioneel beheerder en het afdelingshoofd.

Ook als er nog geen oplossing is, is het voor eindgebruikers fijn om te weten dat aan een oplossing wordt gewerkt.

### STAP 6: Afsluiten incident (afsluiten, evaluatie en rapportage)

Uitvoerder: Behandelaar

- a. Neem preventieve maatregelen om te voorkomen dat deze storing zich opnieuw voordoet. Beschrijf deze maatregelen in de incidentregistratie. Soms resulteert dit in een wijziging en wordt de wijzigingsprocedure gevolgd.
- b. Controleer of er eventueel een kennisitem kan worden gemaakt of moet worden bijgewerkt.
- c. Controleer of, in geval van een (vermoeden van een) informatiebeveiligingsincident, de soort melding en de categorie klopt (beide Beveiligingsincident). De incidentregistratie van deze meldingen moeten minimaal 3 jaar worden bewaard.
- d. Wacht op melder: Laat de melder testen of de maatregel zijn incident oplost.
- e. Meld het incident gereed. Niet afmelden, want dan krijgt de melder geen notificatie.
- e. Als je in een eerder stadium een nieuwsbericht hebt gemaakt: Informeer alle betrokkenen (minimaal degene die tijdens het proces ook zijn geïnformeerd):
  - Maak een nieuwskoppeling (aanpassen nieuwsbericht). Of vraag de Webredactie om dit te doen.



Publicatie op intranet: 18 mei 2022

## Procedure Incidentmeldingen

- Verwijder de storing van TOPdesk.
- Zet het bandje op xxxx uit.
- Stuur een link van het nieuwsbericht naar de functioneel beheerder en het afdelingshoofd.
- De functioneel beheerders informeren hun eindgebruikers en de functioneel beheerder van een gekoppeld informatiesysteem. Een gekoppeld informatiesysteem is ook een eindgebruiker.
- Deel de analyse van het incident met de leverancier en andere partners om te voorkomen dat dit incident zich nog een keer voordoet. Zet ook deze e-mail in TOPdesk.

### Gerelateerde procedures

- Klokkenluidersregeling: Anoniem melden van informatiebeveiligingsincidenten
- Procedure Nieuwe medewerker
- Procedure Wijzigingsbeheer
- Continuïteitsplan

### Interne controle

#### Rapportage

Door CISO aan IBD, binnen 72 uur: Bij een (vermoede van) opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatie verwerkende systemen.

Door FG aan de Autoriteit Persoonsgegevens (AP), binnen 72 uur: Bij een (vermoeden van) een datalek.

In TOPdesk is een online rapportage voor de CISO en de FG beschikbaar. In deze rapportage staan alle beveiligingsincidenten en datalekken van de afgelopen periode. De CISO rapporteert elke maand de opvolging van beveiligingsincidenten en datalekken aan het afdelingshoofd via de Maandinformatie op xxxx. Elk kwartaal rapporteert de CISO over deze beveiligingsincidenten en datalekken aan het MT. Dit staat in de rapportage:

- Aantallen incidenten per categorie.
- Aantallen incidenten per verantwoordelijke (behandelaarsgroep).
- Op tijd of te laat afgehandeld.
- Gemiddelde, maximale en minimale doorlooptijd per categorie.
- Aantal incidenten die geleid hebben tot niet halen van afspraken of het uitvoeren van publieksdiensten (subcategorie Dienstverlening).
- Aantal incidenten met privacy een component (subcategorie Datalek)

Deze rapportage is ook de bron voor de analyse van de incidenten voor bepalen van verbetermaatregelen.



Publicatie op intranet: 18 mei 2022

# Procedure Incidentmeldingen

Elke melding van de categorie Beveiligingsincident moet minimaal 3 jaar bewaard blijven.

## Interne controle

De ICT-coördinator beheert de registratie van (beveiligings)incidenten. Wekelijks overlegt het team I&A over knelpunten bij de behandeling van meldingen.

## Herziening

Frequentie: Elke 3 jaar  
Houdbaar tot: 12 mei 2025  
Vastgesteld door MT: 12 mei 2022  
Auteur: **xxxx**



Publicatie op intranet: 18 mei 2022

# Procedure Incidentmeldingen

## Bijlage 1 Soort melding, categorie en subcategorie

### Soort melding

	Omschrijving	Voorbeelden
<b>Storing</b>	<a href="#">Incident</a>	Ik kan niet meer inloggen.
<b>Informatieverzoek</b>	Verzoek om informatie	Hulpvraag
<b>Feedback</b>	Verstrekken van informatie	Kwetsbaarheidsmelding van een leverancier of de IBD Canary-melding
<b>Aanvraag</b>	Verzoek om een wijziging. Volg de procedure Wijzigingsbeheer.	Extra toegang

NB. Soort melding Beveiligingsincident NIET gebruiken.

### Categorie

Aan elke soort melding kan 1 van de volgende categorieën worden gehangen:

	Omschrijving	Voorbeelden
<b>Beveiligingsincident</b>	<a href="#">Informatiebeveiligingsincident</a>	Als er een 'x' staat in de kolom 'CISO' in <a href="#">Bijlage 2: Incidenten en meldingsniveau matrix</a>
<b>Diensten</b>		
<b>ICT middelen</b>		

NB. Een beveiligingsincident kan ook betrekking hebben op ICT diensten en ICT middelen. Dus: is het geen beveiligingsincident kies dan pas een andere categorie.

### Subcategorie

Voorlopig rapporteren we alleen beveiligingsincidenten. Daarom worden alleen deze hier benoemd.

	Omschrijving	Voorbeelden
<b>Kwetsbaarheid</b>	Een melding van een mogelijk lek in onze systemen	Kwetsbaarheidsmelding van een leverancier of de IBD Canary melding
<b>Datalek</b>	Als er (mogelijk) sprake is van	Misbruik of verlies van persoonsgegevens
<b>Diefstal / verlies</b>	Diefstal of verlies van informatie of informatiedragers.	Telefoon is kwijt USB-stick kwijt
<b>Audit</b>	Bevindingen uit pentesten, zelfevaluaties, zelfcontroles, interne en externe audits.	Bevinding uit de pentest
<b>Autorisatie</b>	(Bevindingen na een) controle op de toegangsrechten. Verkeerde rechten uitgedeeld.	Controle toegangsrechten Iemand kan niet inloggen
<b>Dienstverlening</b>	Incident dat heeft geleid tot niet halen van afspraken of het uitvoeren van publieksdiensten	



Publicatie op intranet: 18 mei 2022

## Procedure Incidentmeldingen

<b>Overig</b>	Mogelijk dat hierbinnen nieuwe subcategoriën worden benoemd.	Storing in de backup Melding van phishing e-mail
---------------	--	---

### Bijlage 2: Incidenten en meldingsniveau matrix

In onderstaande tabel staat wie geïnformeerd wordt over een incidentmelding.

Deze tabel is overgenomen uit de [Handreiking Incident- en response management \(IBD\)](#)

- Helpdesk: Incidenten die door gebruiker en/of beheerder worden gemeld bij helpdesk.
- CISO: Incidenten die door helpdesk worden gecategoriseerd als Beveiligingsincident.
- Directie: Incidenten die door CISO worden gemeld bij directie. (X) is afhankelijk van de ernst.

Gebruikersincidenten		Niveau van melding		
Categorie	Mogelijk incident	Helpdesk	CISO	Directie
Onopzettelijk foutief handelen	Door fouten in handleiding of procedure	X		
	Door foutgevoelige bediening	X		
	Onzorgvuldige omgang met wachtwoorden	X		
Opzettelijk foutief handelen	Niet volgen van voorschriften	X	X	(X)
	Fraude of diefstal	X	X	X
	Ongeautoriseerde toegang door medewerker	X	X	X
	Kraken of omzeilen toegang door medewerkers of een buitenstaander			
Technisch falen van apparatuur	Storing in apparatuur	X	P1 of P2	
	Wegvallen elektrische spanning of spanningsschommelingen	X	X	X
	Wateroverlast	X	X	X
	Uitval netwerkverbinding door aanval met grote hoeveelheden data	X	X	X
Menselijke omgang met apparatuur	Bedieningsfouten	X		
	Opzettelijke wijzigingen	X	X	(X)
	Beschadiging of vernieling van apparatuur	X	X	X
	Apparatuur blijkt niet geregistreerd	X		
	Geregistreerde apparatuur blijkt niet aanwezig	X	X	
Problemen met programmatuur	Fouten in programmatuur	X		
	Ongeautoriseerde wijzigingen in programmatuur	X	X	
	Opzettelijk introduceren van een virus door medewerker	X	X	X
	Inbrengen van virus door middel van niet gescreende programmatuur	X	X	X
	(On)opzettelijk ongeautoriseerd gebruik	X	X	



Publicatie op intranet: 18 mei 2022

## Procedure Incidentmeldingen

Gebruikersincidenten		Niveau van melding		
Categorie	Mogelijk incident	Helpdesk	CISO	Directie
	Gebruik van ongeautoriseerde programmatuur	X	X	
	Wijziging door medewerker	X	X	X
	Illegaal kopiëren	X	X	X
	Diefstal van programmatuur	X	X	X
Omstandigheden op de werkplek	Uitval van elektriciteit	X	X	X
	Wateroverlast door lekkage	X	X	X
	Ongewenste trillingen	X		
	Kortsluiting	X		
	Ongeoorloofde toegang tot computerruimte	X	X	X
	Uitgifte sleutels aan ongeautoriseerde	X	X	X
Identificatie en bevoegdheden van gebruikers	Geen eenduidige gebruiker bij een user-ID geconstateerd	X	X	
	Ongeautoriseerde toegang door medewerker	X	X	X
	Er komen gebruikers voor die niet meer bevoegd zijn (ex-medewerkers)	X	X	
	Vraagtekens bij bevoegdheden van bepaalde gebruikers of beheerders	X	X	
Gegevensdragers	Zoekraken gegevensdragers	X	X	X
	Diefstal van gegevensdragers	X	X	X
	Beschadiging gegevensdragers	X		
	Onleesbaarheid van gegevensdragers	X		
Gegevens	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
	Ongeautoriseerde toegang tot gegevens	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 gemeente	X	X	X



Publicatie op intranet: 18 mei 2022

# Procedure Incidentmeldingen



Publicatie op intranet: 18 mei 2022

# Procedure Incidentmeldingen

## Bijlage 3: Incident Impact bepaling

**LET OP: de tabel bevat slechts voorbeelden.**

Om de impact van een incident te bepalen, kiest je altijd de hoogst voorkomende waarde van de getroffen categorieën. Is de impact Hoog, dan deel je de melding met de ICT-coördinator en de CISO.

Onderwerp	Laag	Midden	Hoog
<b>Aantal getroffen medewerkers</b>	<10	<100	>100
<b>Apparatuur werkt niet</b>	Enkele apparaten uitgevallen.	Meerdere apparaten uitgevallen.	Meeste apparaten uitgevallen.
<b>Apparatuur werkt niet</b>	De apparatuur kan eenvoudig vervangen worden.	De apparatuur ondersteunt primaire processen en is moeilijk vervangbaar.	De dienstverlening van de gemeente komt voor langere tijd tot stilstand.
<b>Programmatuur werkt niet</b>	Software die de secundaire processen ondersteunt is uitgevallen.	Software die de primaire processen ondersteunt is uitgevallen.	Software die de primaire processen ondersteunt is uitgevallen en kan langere tijd niet gebruikt worden.
<b>Gegevens worden gekopieerd, versleuteld dan wel vernietigd</b>	Gegevens die secundaire processen ondersteunen.	Gegevens die primaire processen ondersteunen.	Gegevens die organisatie overstijgend in ketens verwerkt worden.
<b>Organisatieprocessen</b>	Het incident blijft beperkt tot een enkele ondersteunende afdeling.	Het incident heeft impact op een primair proces, de publieksbalie moet gesloten worden.	Het incident overstijgt de organisatie (lokaal/regionaal) of er is impact op de buitenruimte.
<b>Omgeving</b>	Het incident beperkt zich tot een fysieke afdeling binnen het gemeentehuis.	Het incident treft meerdere afdelingen binnen een gemeentehuis.	Het incident breidt zich uit naar de buitenruimte en er ontstaat maatschappelijke onrust.
<b>Diensten</b>	Het incident beperkt zich tot lokale applicaties en systemen.	Het incident breidt zich uit naar of vindt plaats bij off-premise leveranciers en diensten.	Het incident breidt zich uit en keten afhankelijke diensten komen in gevaar.
<b>Impact op betrokkenen</b>	Het incident leidt niet tot enige schade voor betrokkenen.	Het incident leidt tot een klein risico voor betrokkenen.	De groep van betrokkenen is groot of het incident leidt tot een hoog risico voor betrokkenen.
<b>Kans op reputatieschade</b>	Geen kans op reputatieschade.	De reputatieschade beperkt zich tot lokale afdelingen en afdelingsmanagers.	De reputatieschade is hoog met de kans dat het college valt.



Publicatie op intranet: 18 mei 2022

## Procedure Incidentmeldingen

Onderwerp	Laag	Midden	Hoog
<b>Financiële impact</b>	De schade als gevolg van het incident is op te vangen binnen de begroting van een afdeling.	De schade als gevolg van het incident is op te vangen binnen de begroting van de organisatie.	De schade als gevolg van het incident is niet meer op te vangen binnen de begroting of getroffen voorzieningen.
<b>Werk om te herstellen is arbeidsintensief</b>	Het terugzetten van back-ups is voldoende om weer up en running te komen.	Back-ups hebben afhankelijkheden en deze moeten gecoördineerd en gecontroleerd worden.	De inspanning om te herstellen legt grote druk op de hele organisatie, externe ondersteuning is nodig.
<b>Snelheid van toename incident</b>	Het incident beperkt zich tot de getroffen apparaten en breid zich niet verder uit.	Het incident breidt zich uit naar andere apparaten en breid zich langzaam uit als er geen actie ondernomen wordt.	Het incident breidt zich snel verder uit en heeft in korte tijd de hele dienstverlening onmogelijk gemaakt.
<b>Ketenafhankelijkheid</b>	De geraakte processen zijn geïsoleerd en blijven binnen de afdeling waar het incident optreedt.	De geraakte processen beïnvloeden andere afdelingen binnen de organisatie.	Ketenafhankelijkheden zijn organisatie overstijgend regionaal en/of nationaal.
<b>Beschikbaarheid bedrijfsprocessen</b>	De geraakte productieprocessen ondervinden geen of zeer weinig hinder van het incident.	De dienstverlening van de primaire producten en diensten ondervindt hinder en loopt vertraging op.	De primaire producten en diensten zijn voor lange tijd niet beschikbaar en de dienstverlening aan inwoners en bedrijven stopt.



Publicatie op intranet: 2 februari 2024

# Procedure Wijzigingsbeheer

Wijzigingsbeheer zorgt ervoor dat we wijzigingen op de ICT-infrastructuur efficiënt en effectief doorvoeren. Met zo weinig mogelijk verstoring van de kwaliteit van de (interne) dienstverlening. Wijzigingsbeheer zorgt er ook voor dat beveiligingsinstellingen van de ICT-infrastructuur niet ongecontroleerd en ongeautoriseerd gewijzigd kunnen worden. En dat we aan de beveiligingsnormen blijven voldoen. Met deze procedure volgen we de procesbeschrijving Change Management van het ITIL beheerframework. Deze procedure beschrijft de taken en verantwoordelijkheden van de betrokkenen bij een wijziging.

## Verantwoordelijkheden

- Leidinggevende:
  - is verantwoordelijk voor de beschikbaarheid van voldoende resources om wijzigingen op tijd te kunnen implementeren.
  - autoriseert het in productie nemen van een grote wijziging.
  - besluit of gebruik wordt gemaakt van een terugvalscenario.
- Leidinggevende team I&A:
  - keurt de classificatie van een wijzigingsvoorstel tot Noodwijziging goed.

## Begrippen

### Configuratie item (CI)

Een configuratie item is een programma of apparaat dat gewijzigd wordt. Voorbeelden zijn: telefoon, server, informatiesysteem, besturingssysteem, back-upconfiguratie etc.

### Onderhoudsvenster

Het onderhoudsvenster bepaalt wanneer wijzigingen met impact voor eindgebruikers mogen worden doorgevoerd. Afwijken van dit onderhoudsvenster mag alleen in overleg met de proceseigena(a)r(en). Dit zijn de eigenaren van de processen die (mogelijk) hinder ondervinden van het onderhoud.

De onderhoudsvensters zijn als volgt:

- Dinsdag 17.00-24.00 uur (vooral beveiligingsupdates).
- Vrijdag 17.00-24.00 uur.
- Zaterdag 0.00-24.00 uur.

### OTAP(E)

OTAP staat voor ontwikkelen, testen, accepteren en productie. Soms wordt hier een E (van Educatie) aan toegevoegd. Deze wijzigingsprocedure volgt de OTAPE-methodiek. Afhankelijk van de wijzigingsaanvraag wordt slechts een deel van deze methodiek gevolgd.



Publicatie op intranet: 2 februari 2024

# Procedure Wijzigingsbeheer

## Vormvrij

Om de werking van de procedure aantoonbaar te maken, vindt er verslaglegging plaats. De vorm waarin dat gebeurt is niet voorgeschreven. Soms volstaat een notitie in TOPdesk. Soms is een uitgebreid testverslag nodig. Dit ter beoordeling van de Wijzigingsbeheerder.

## Wijziging

Een wijziging is de toevoeging, verandering of verwijdering van alles dat een effect kan hebben op ICT-dienstverlening. Het gaat hierbij om wijzigingen van software, hardware en ICT-diensten. En de gevolgen die dit heeft op documentatie, architecturen en andere instrumenten. We onderkennen een aantal **soorten** wijzigingen.

### Standaardwijziging

Dit zijn routinematige beheertaken, die procedurematig (gestandaardiseerd) worden uitgevoerd. Voor deze wijzigingen zijn door het MT procedures vastgesteld of er zijn kennisitems voor gemaakt. Deze wijzigingen worden niet voorgelegd aan de Wijzigingsadviescommissie.

### Niet-standaard wijzigingen

Dit betreft alle wijzigingsverzoeken die afwijken van de standaard en waarvoor nog geen afspraken of kennis items zijn gemaakt. Daarbij wordt onderscheidt gemaakt in urgentie. De urgentie is een inschatting van de aanvrager en de helpdeskmedewerker.

### Noodwijziging

Dit type wijziging is een oplossing voor incidenten bij primaire bedrijfsprocessen, die een belangrijke impact hebben en acuut de voortgang belemmeren. Noodwijzigingen wijken af van de normale procedures, omdat voor dit soort wijzigingen de benodigde middelen en capaciteit meteen moeten worden vrijgemaakt.

De coördinator ICT bepaalt, samen met het afdelingshoofd, welke stappen van de wijzigingsprocedure worden overgeslagen. De wijziging wordt wel altijd getest. De Coördinator ICT registreert de procesgang rondom urgente wijzigingsvoorstellen in TOPdesk. Hiermee kan hij zich verantwoorden aan de Wijzigingsadviescommissie en het afdelingshoofd Bestuur en Organisatie.

## Wijzigingsadviescommissie

Het wekelijks teamoverleg I&A is ook de commissie die alle niet-standaard wijzigingen beoordeelt, (niet) accepteert en inplant. Voor spoedwijzigingen wordt een extra Wijzigingsadviescommissie bijeengeroepen. De ICT coördinator is voorzitter van dit overleg.



Publicatie op intranet: 2 februari 2024

# Procedure Wijzigingsbeheer

## Wijzigingsbeheerder

De wijzigingsbeheerder is degene die de uitvoering van de wijziging coördineert en bewaakt. Dit kan een systeembeheerder of een functioneel beheerder zijn. Dit is de eigenaar (Behandelaar) van de wijziging.

## Processtappen

[P\\_Wijzigingsbeheer.vsdX](#)

## Aanleiding (detectie)

Aankondiging of wens tot wijziging van hardware, software of ICT-dienst.

## Hulpmiddelen

TOPdesk:

- Wijzigingenregistratie en -communicatie
- Overzicht configuratie items (Asset Management)
- Agenda Wijzigingsadviescommissie (Rapport Wijzigingscommissie – Wijzigingen)
- Wijzigingskalender (Kalender in TOPdesk - niet zichtbaar voor medewerkers)

## STAP 1: Melden wijziging

Uitvoerder: Aanvrager

Het volgende wordt gemeld in TOPdesk (tussen haakjes staat de **bevoegd aanvrager**):

1. Aanvraag van een nieuw of een uitbreiding van een bestaand informatiesysteem (**afdelingshoofd vak-afdeling**).
2. Aankondiging van een wijziging van een informatiesysteem (**functioneel beheerder**).
3. Aanvraag waarbij afgeweken wordt van bestaand beleid (**afdelingshoofd Bestuur en organisatie**)
4. Overige wijzigingsverzoeken (**1<sup>e</sup> medewerker of teamleider**).

In [xxxx@lochem.nl](mailto:xxxx@lochem.nl):

5. Aankondiging van wijzigingen van hardware, systeemsoftware of ICT-diensten (**leverancier**).
6. Instroom-, doorstroom- en uitstroommeldingen van (**ADP Workforce**).
7. Kwetsbaarheidsmeldingen (**Informatiebeveiligingsdienst, leverancier**).

**AFSPRAAK:** De functioneel beheerder beoordeelt de releasenotes, voordat deze in productie worden geïnstalleerd. Blijkt uit de releasenotes dat de kans groot is, dat het informatiesysteem langere tijd niet beschikbaar is of invloed heeft op beveiligingsmaatregelen (inloggen, autorisatie, gebruikersbeheer), dan wordt de wijziging gemeld in TOPdesk en wordt deze procedure gevolgd.



Publicatie op intranet: 2 februari 2024

# Procedure Wijzigingsbeheer

## STAP 2: Classificeren aanvraag

Uitvoerder: Helpdeskmedewerker 1<sup>e</sup> lijn

- a. Controleer of de aanvrager de juiste [bevoegdheid](#) heeft om deze wijziging aan te vragen. Zo niet, vraag dan de aanvrager dit te herstellen.
- b. Relateer de wijziging aan **incidenten** die door deze wijziging worden opgelost.
- c. Koppel de aanvraag aan het **configuratie item** waarop de wijziging betrekking heeft. Voer het configuratie-item op, als deze nog niet bestaat.
- d. Kijk of er een kennis item aanwezig of sjabloon is om deze wijziging door te voeren.
- e. Classificeer de wijziging (categorie, subcategorie, sjabloon, noodwijziging, standaard of niet-standaard etc.)
- f. Bepaal de behandelaarsgroep of behandelaar. Noteer eventuele opmerkingen voor de volgende behandelaar (vink 'onzichtbaar voor aanmelder' aan).
- g. Niet-standaard wijziging: Controleer of de aanvraag voldoende informatie bevat om in de Wijzigingsadviescommissie te bespreken. Haal eventueel aanvullende informatie op bij de aanmelder.

Ligt de gewenste implementatiedatum voor de eerstvolgende Wijzigingsadviescommissie, dan is een versnelde procedure nodig. Informeer de ICT-coördinator voor een extra Wijzigingsadviescommissie.

**AFSPRAAK:** *Binnen 24 uur nadat de wijziging is aangevraagd, is deze stap afgerond.*

**AFSPRAAK:** *Bij een hoge kans op misbruik en een hoge kans op schade worden patches uiterlijk binnen een week geïnstalleerd. In afwachting van het installeren van patches worden op basis van een expliciete risicoafweging mitigerende maatregelen genomen en geregistreerd.*

## STAP 3: Accepteren en plannen niet-standaard wijzigingen

Uitvoerder: Wijzigingsadviescommissie, Wijzigingsbeheerder

- a. Beoordeel elke wijziging op de agenda.
- b. Accepteer de wijziging, of niet.
- c. Noteer de beoordeling (met gevolgen en risicoafweging) in de TOPdesk melding.

**AFSPRAAK:** *Functioneel beheerders zitten niet in de Wijzigingsadviescommissie. Soms gaat de wijziging gaat over een informatiesysteem. Dan overlegt een medewerker van I&A eerst met de functioneel beheerder. En neemt de bevindingen mee naar de Wijzigingsadviescommissie. De functioneel beheerder kan ook uitgenodigd worden voor het overleg.*

Geaccepteerde wijzigingen:

Keur de aanvraag goed. Pas eventueel behandelaar (wijzigingsbeheerder) en implementatiedatum aan. De wijziging komt vanzelf op de wijzigingskalender.



Publicatie op intranet: 2 februari 2024

## Procedure Wijzigingsbeheer

Niet geaccepteerde wijzigingen

Wijs de aanvraag af. Beargumenteer naar de aanvrager waarom de wijziging niet geaccepteerd wordt.

### STAP 4: Uitvoeren wijziging

Uitvoerder: Wijzigingsbeheerder

Voer de wijziging door. Houd daarbij rekening met het volgende (voor zover van toepassing):

- Volg de instructies in het TOPdesk-sjabloon of -kennisitem.
- Informeer of leer eindgebruikers over de wijzigingen (bij voorkeur via Leo).
- Informeer de functioneel beheerder van een gekoppeld informatiesysteem. Zij informeren op hun beurt hun eindgebruikers.
- Pas eventuele documentatie (sjablonen, Leo-teksten, kennisitems, etc.) aan.

Bij nieuwe informatiesystemen of uitbreiding van bestaande informatiesystemen geldt daarnaast:

- Installeer de wijziging in de testomgeving (meestal door de leverancier).
- Configureer de wijziging in de testomgeving (meestal door of samen met de leverancier).
- Maak een testplan (wat ga je testen), een terugvalscenario en een testverslag.
- Noteer eventuele bevindingen in het testverslag.
- Geef de testomgeving vrij om over te zetten naar productie (acceptatie testomgeving).
- Installeer de wijziging in de productieomgeving (meestal door de leverancier).
- Test de productieomgeving op hoofdlijnen (volgens het testplan).
- Laat de leidinggevende de productieomgeving vrijgeven voor gebruik (acceptatie productieomgeving).
- Zorg voor beschikbaarheid en ondersteuning/opleiding in de nazorgfase.
- Verwijder eventuele productiegegevens die voor testdoeleinden zijn gebruikt.

Gaat het niet goed? Activeer dan in overleg met het afdelingshoofd het terugvalscenario.

**AFSPRAAK:** Zorg dat minimaal het testverslag, de test- en productie-acceptatie aantoonbaar (vormvrij) aanwezig is in TOPdesk. In een testverslag staan ook printscreens die aantonen dat een test succesvol is uitgevoerd. Staan de documenten elders? Noteer dan het zaaknummer of de plek in TOPdesk. Wijk je af van deze procedure, dan meld je dat (met de reden) in TOPdesk.

**AFSPRAAK:** In de productieomgeving worden geen updates getest. Behalve als daarvoor door het afdelingshoofd expliciet toestemming is gegeven. Deze toestemming sla je (vormvrij) op.

**AFSPRAAK:** Updates worden (door de leverancier) altijd getest, voordat zij in productie gebracht worden. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken.



Publicatie op intranet: 2 februari 2024

# Procedure Wijzigingsbeheer

## STAP 5: Afsluiten

Uitvoerder: Systeem- / Netwerkbeheerder

Na implementatie verwerk je de wijziging in de administraties:

- Actualiseer de gewijzigde configuratie items.
- Controleer of elke gerelateerde incidentmelding ook echt is opgelost. En meld deze gereed.
- Kan er een standaard-wijziging (of kennisitem) van worden gemaakt? Maak deze dan aan.
- Heeft de wijziging gevolgen voor de uitwijkconfiguratie? Geef dit dan door aan Infinity BV.
- Heeft de wijziging gevolgen voor de beveiliging? Geef dit dan door aan GroupSecure.

## STAP 7: Evalueren niet-standaard wijziging

Uitvoerder: Wijzigingsadviescommissie, wijzigingsbeheerder

- a. Bespreek in de WAC eventueel afgeronde niet-standaard wijzigingen:
  - Heeft de wijziging het beoogde doel bereikt?
  - Zijn de gebruikers tevreden met het resultaat?
  - Heeft de wijziging tot nieuwe incidenten/nevenverschijnselen geleid?
  - Is er nog extra nazorg nodig?
  - Zijn de geraamde kosten en inspanningen niet overschreden?Beschrijf de evaluatie in de TOPdesk-melding.
- b. Wijzig de status van de aanvraag in Geëvalueerd (bij een positieve evaluatie) of In behandeling (bij extra nazorg, of andere corrigerende maatregelen).

## Gerelateerde procedures

- Back-up en recoverybeleid (nog op te stellen)
- Procedure Nieuwe medewerker
- Procedure Incidentmeldingen
- Diverse kennisitems



Publicatie op intranet: 2 februari 2024

# Procedure Wijzigingsbeheer

## Interne controle

### Rapportage

In TOPdesk is een rapportage beschikbaar. In deze rapportage staan alle wijzigingsmeldingen van de afgelopen periode. Elk kwartaal rapporteert team I&A over deze wijzigingen aan het MT.

Wijzigingsvoorstellen voor het SIO worden door de Coördinator ICT gedeeld met de Informatiemanager om op de agenda te plaatsen.

### Interne controle

De ICT-coördinator ziet erop toe dat de wijzigingsprocedures worden gehandhaafd en bewaakt de voortgang van de afhandeling van wijzigingen.

De ICT coördinator controleert periodiek, in elk geval voor elke dinsdag, of er nog patches ontbreken tegen bekende (CVE) kwetsbaarheden.

### Herziening

Frequentie: Elke 3 jaar  
Houdbaar tot: 1 februari 2027  
Vastgesteld door MT: 1 februari 2024  
Auteur: **xxxx**