

Voorbeeld

Incidentmanagement en response beleid

Een operationeel kennisproduct ter ondersteuning van de implementatie van de Baseline Informatiebeveiliging Overheid (BIO)

Colofon

### Naam document

Voorbeeld incidentmanagement en response beleid

### Versienummer

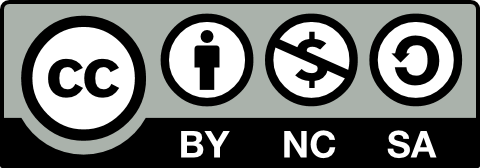
2.0

### Versiedatum

Januari 2019

### Versiebeheer

Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).



Vereniging van Nederlandse Gemeenten / Informatiebeveiligingsdienst voor gemeenten (IBD) (2018)

Tenzij anders vermeld, is dit werk verstrekt onder een Creative Commons Naamsvermelding-Niet Commercieel-Gelijk Delen 4.0 Internationaal licentie. Dit houdt in dat het materiaal gebruikt en gedeeld mag worden onder de volgende voorwaarden: Alle rechten voorbehouden. Verveelvoudiging, verspreiding en gebruik van deze uitgave voor het doel zoals vermeld in deze uitgave is met bronvermelding toegestaan voor alle gemeenten en overheidsorganisaties.

Voor commerciële organisaties wordt hierbij toestemming verleend om dit document te bekijken, af te drukken, te verspreiden en te gebruiken onder de hiernavolgende voorwaarden:

1. De IBD wordt als bron vermeld;
2. Het document en de inhoud mogen commercieel niet geëxploiteerd worden;
3. Publicaties of informatie waarvan de intellectuele eigendomsrechten niet bij de verstrekker berusten, blijven onderworpen aan de beperkingen opgelegd door de IBD en / of de Vereniging van Nederlandse Gemeenten;
4. Iedere kopie van dit document, of een gedeelte daarvan, dient te zijn voorzien van de in deze paragraaf vermelde mededeling.

Wanneer dit werk wordt gebruikt, hanteer dan de volgende methode van naamsvermelding: “Vereniging van Nederlandse Gemeenten / Informatiebeveiligingsdienst voor gemeenten”, licentie onder: CC BY-NC-SA 4.0.

Bezoek <http://creativecommons.org/licenses/by-nc-sa/4.0> voor meer informatie over de licentie.

### Rechten en vrijwaring

De IBD is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan de IBD geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. De IBD aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

### Met dank aan

De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

### Wijzigingshistorie

|  |  |  |
| --- | --- | --- |
| Versie | Datum | Wijziging / Actie |
| 1 | Juli 2013 | Initiele versie |
| 1.01 | Augustus 2015 | Kleine tekstuele wijzigingen |
| 1.1 | December 2015 | Aanpassing ivm WBP |
| 1.1.1 | Augustus 2016 | Taskforce BID verwijderd |
| 2.0 | December 2018 | BIO Update , AVG update |

Over de IBD

De IBD is een gezamenlijk initiatief van alle Nederlandse Gemeenten. De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en richt zich op (incident)ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD ondersteunt gemeenten bij hun inspanningen op het gebied van informatiebeveiliging en privacy / gegevensbescherming en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruikmaken van de producten en de generieke dienstverlening van de IBD.

De IBD is ondergebracht bij VNG Realisatie.

Leeswijzer

Dit product is een nadere uitwerking voor gemeenten van de Baseline Informatiebeveiliging Overheid (BIO). De BIO is eind 2018 bestuurlijk vastgesteld als gezamenlijke norm voor informatiebeveiliging voor alle Nederlandse overheden.

**Doel**

Het doel van dit document is om een invulling van beleidsuitgangspunten te geven voor het incidentmanagement en response beleid.

**Doelgroep**

Dit document is van belang voor de CISO, de systeemeigenaren, applicatiebeheerders en de ICT-afdeling.

**Relatie met overige producten**

* Baseline Informatiebeveiliging Overheid (BIO)
* Informatiebeveiligingsbeleid van de gemeente
* Handreiking patchmanagement voor gemeenten
* Handreiking proces wijzigingsbeheer
* Handreiking proces configuratiebeheer
* Handreiking patchmanagement voor gemeenten

Verwijzingen naar de Baseline Informatiebeveiliging voor de Overheid (BIO)

6.1.1.1 Verantwoordelijkheden zijn vastgelegd door leiding van de organisatie

7.1.2.1 Alle medewerkers zijn gewezen op hun verantwoordelijkheid omtrent informatiebeveiliging

7.2.2.1 Alle medewerkers hebben de verantwoordelijkheid om bedrijfsinformatie te beschermen en kennen de regels en verplichtingen

9.4.4.2 Het gebruik van systeemhulpmiddelen wordt gelogd

11.1.2.1 Waarschuwingen van concrete beveiligingsrisico’s worden gedeeld met relevante collega’s

12.3.1.2 Risicoafweging voor maximale dataverlies en maximale hersteltijd

12.4.2 Bescherming van informatie in logbestanden

12.4.2.2 Risicoafweging voor bewaarperiode van logging

12.6.1 Beheer van technische kwetsbaarheden

15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten

H16 Beheer van informatiebeveiligingsincidenten

### Wat is er veranderd ten opzichte van de BIG?

Voor logging geldt dat de logging over systeemhulpmiddelen een halfjaar beschikbaar is voor onderzoek en dat logbestanden beschermd moeten worden tegen vervalsing en onbevoegde toegang. Tevens moeten concrete beveiligingsrisico’s nu worden doorgestuurd naar relevante collega’s binnen het beveiligingsdomein (versturen naar de IBD voldoet).

Managementsamenvating

Deze handreiking beschrijft de beleidsuitgangspunten en bijhorende processtappen voor het incidentmanagement- en responsbeleid. Omdat 100% informatieveiligheid niet bestaat zullen incidentenplaatsvinden. Het hebben van een goed incidentmanagement- en responsproces zal de impact daarvan verkleinen, omdat adequaat gereageerd kan worden en de schade en impact hierdoor minimaal kunnen blijven. Daarnaast leidt het proces dat lering wordt getrokken van incidenten, waardoor de kans op herhaling ook wordt verkleind. Alle medewerkers zijn verantwoordelijk voor informatiebeveiliging en dienen een incident te herkennen en weten waar ze dat moeten melden.

Er zijn verschillende type incidenten die allemaal een prioritering dienen te krijgen, afhankelijk van de impact en de urgentie van het incident dient er een prioritering aan gehangen te worden. Het eerste uur na ontdekking van een incident kan cruciaal zijn, er moet zo min mogelijk impact zijn van het incident zonder dat er informatie verloren gaat. Dit is namelijk nodig om later een goed onderzoek te kunnen doen naar de oorzaak van het incident.

Een incident response-actie bestaat uit de volgende stappen:

* identificatie
* schade indamming (insluiting en beperking)
* remediatie en herstel
* kennisgeving aan betrokkene
* rapportage en evaluatie

Inhoudsopgave

[1. Inleiding 7](#_Toc14781573)

[1.1. Doelstelling incidentmanagement 7](#_Toc14781574)

[1.2. De indeling van het document is als volgt: 7](#_Toc14781575)

[2. Incidentmanagement en response stappen 8](#_Toc14781576)

[2.1. Opzetten incidentmanagement 8](#_Toc14781577)

[2.2. Identificatie 8](#_Toc14781578)

[2.3. Schade indamming 8](#_Toc14781579)

[2.4. Remediatie en herstel 9](#_Toc14781580)

[2.5. Kennisgeving 9](#_Toc14781581)

[2.6. Rapportage en evaluatie 9](#_Toc14781582)

[2.7. Hoe te gebruiken 9](#_Toc14781583)

[3. Aandachtspunten 11](#_Toc14781584)

[3.1. Logging 11](#_Toc14781585)

[3.2. Personeel 11](#_Toc14781586)

[3.3. Voorbereiding 11](#_Toc14781587)

[3.4. Gouden uur 12](#_Toc14781588)

[3.5. Gouden tips 12](#_Toc14781589)

[4. Incident Prioritering Leidraad 13](#_Toc14781590)

[4.1. Incident urgentie (categorieën) 13](#_Toc14781591)

[4.2. Incident impact (categorieën) 14](#_Toc14781592)

[4.3. Incident Prioriteringsklassen 15](#_Toc14781593)

[Bijlage 1: Incidentmanagement en response beleid stappenplan en sjabloon 17](#_Toc14781594)

[Bijlage 2: Incidentenprocedure informatiebeveiliging 27](#_Toc14781595)

[Bijlage 3: Incidenten en meldingsniveau matrix 28](#_Toc14781596)

[Bijlage 4: Definities 31](#_Toc14781597)

[Bijlage 5: Incidentmanagement en response beleid gemeente <gemeente> 33](#_Toc14781598)

# Inleiding

Incidentmanagement is bij gemeenten vaak in meer of mindere mate uitgewerkt. Het bevat het identificeren, oplossen en het leren van een incident, zodat de impact en kans op herhaling minimaal is. Het gaat bij informatiebeveiliging om informatiebeveiligingsincidenten die betrekking hebben op de informatievoorziening. Vaak spreekt men ook over Computer Security Incidentmanagement. Waar in dit document gesproken wordt over Computer Security Incidentmanagement bedoelen we hetzelfde als incidentmanagement en response of in het kort incidentmanagement. Het primaire doel is de ontwikkeling van een goed begrepen en voorspelbare reactie op schadelijke gebeurtenissen in de meest brede zin van het woord.

Gemeenten moeten zich bewustzijn van hun verantwoordelijkheden als het gaat om de bescherming van deze informatie ten behoeve van hun burgers en ketenpartners. Deze verantwoordelijkheid strekt zich uit tot het hebben van een draaiboek voor ‘wat te doen, als er iets misgaat’.

## Doelstelling incidentmanagement

Incidentmanagement is zo belangrijk omdat 100% beveiligen niet bestaat en los daarvan: niet alle incidenten zijn te voorkomen. Het is niet de vraag óf er iets gaat gebeuren maar wanneer. De belangrijkste te verwachte incidenten kunnen van te voren bedacht worden en de bijpassende reactie en escalatieprocedure kan dus ook van te voren uitgewerkt en geoefend worden. Het incidentmanagement proces heeft dan ook als doel om verstoringen zo snel mogelijk te verhelpen en optreding in de toekomst te verhelpen. Als er sprake is van uitbesteding dan dienen er goede contractuele afspraken gemaakt te worden dat de leverancier op basis van prioriteit kwetsbaarheden snel moet oplossen.

Incidenten staan vaak niet op zichzelf en kunnen een uitwerking hebben naar andere ketenpartners. Sommige incidenten doen zich niet bij één gemeente voor maar bij meerdere. Een incident moet behalve intern opgelost soms ook extern geëscaleerd worden zodat anderen gewaarschuwd kunnen worden en daarmee de impact van het incident zo klein als mogelijk gehouden kan worden. Extern escaleren gebeurt naar de IBD, zij hebben het overzicht, de contacten en de middelen om andere (keten)partners en gemeenten snel te kunnen waarschuwen en ook hebben zij een directe ingang bij het Nationaal Cyber Security Centrum (NCSC).

## De indeling van het document is als volgt:

Hoofdstuk 2 gaat over het incidentmanagement en responseproces waarin is toegelicht dat het proces bestaat uit: identificatie, indamming, herstel, kennisgeving en rapportage. Daarnaast is er een stuk opgenomen over de meldingen en wie je wanneer moet inlichten. Hoofdstuk 3 beschrijft verschillende aspecten die bij dit proces komen kijken zoals logging en het gouden uur. Hoofdstuk 4 gaat in op de verschillende prioritering die bij incidenten komen kijken. Afhankelijk van de urgentie en impact dient een incident als hoog of juist lager te worden geprioriteerd.

# Incidentmanagement en response stappen

Een incident, in het kader van incidentmanagement, is een gebeurtenis die de bedrijfsvoering negatief kan beïnvloeden. Incidentmanagement is het geheel van organisatorische maatregelen dat ervoor moet zorgen dat een incident adequaat gedetecteerd, gemeld en behandeld wordt om daarmee de kans op uitval van bedrijfsvoeringsprocessen of schade ontstaan als gevolg van het incident te minimaliseren, dan wel te voorkomen.

## Opzetten incidentmanagement

Een succesvol incidentmanagement en responsebeleidreactie bestaat uit een aantal te doorlopen stappen. Deze stappen zijn voor iedere incident gelijk, alleen in de details zitten de verschillen.

De volgende informatie is bedoeld als een algemene checklist van de stappen die een gemeente kan nemen wanneer een incident wordt ontdekt. Er bestaan andere checklists en deze kunnen ook al in gebruik zijn. Deze checklist kan nuttig zijn voor iedereen, als een herziening van paraatheid of als een routekaart voor ontwikkeling. De eigenaar van het incidentmanagement en response proces is de incidentmanager. De helpdesk heeft een nadrukkelijke rol bij het ontwikkelen van incident response reacties en bij de voorbereiding daarop.

Belangrijk is dat incidenten enuitgevoerde activiteiten worden vastgelegd voor latere evaluatie, woordvoering, bewijslast en dergelijke.

Een incident response-actie bestaat uit de volgende stappen:

* identificatie
* schade indamming (insluiting en beperking)
* remediatie en herstel
* kennisgeving
* rapportage en evaluatie

Onderstaande stappen zijn in detail beschreven in het incidentmanagement en response beleid- stappenplan en -sjabloon, zie bijlage A.

## Identificatie

Controleer of er een kwetsbaarheid aanwezig is en/of een incident daadwerkelijk heeft plaatsgevonden. Deze activiteit omvat normaliter de systeembeheerder en eindgebruiker, maar kan ook het gevolg zijn van proactieve detectie van incidenten door de ICT-beveiliging of het systeembeheer of doordat bij de controle van de logging iets naar boven komt. Indien wordt vastgesteld dat het inderdaad een kwetsbaarheid of incident is, dan moeten de betreffende instanties gewaarschuwd worden.

## Schade indamming

Nadat het incident is opgemerkt en gemeld gaat de servicedesk ermee aan de slag. De incidentmanager (soms gewoon een helpdeskmedewerker) moet gaan handelen om de schade van het incident te beperken. De incidentmanager zal waar nodig een team aanstellen om het incident te verhelpen en zal hiervoor soms ook de CISO & FG nodig hebben. Bij grote informatiebeveiligingsincidenten zal de manager van de bedrijfsvoering of de gemeentesecretaris een belangrijke rol spelen en zal de CISO in de meeste gevallen de teamleider worden. Dit team is belast met het beperken van verdere schade als gevolg van het incident en kan de IBD inschakelen voor advies. Start een grondige beoordeling van de aard en omvang van het incident, stel vast wat de schade is en stel bewijsmateriaal veilig. Bepaal of het datalek onder de AVG valt, en volg het datalekkenproces. Als bekend is dat het een datalek is, maar nog niet alle gegevens over het datalek bekend zijn, dan kan beslist worden een voormelding bij de AP te doen en later deze in te trekken of verder aan te vullen.

## Remediatie en herstel

Neem maatregelen om de oorzaak van het incident te blokkeren of te verwijderen, verminder de impact door verdere blootstelling van de gevoelige gegevens te voorkomen, maak een start om de bedrijfsprocessen te herstarten als deze gestopt waren als gevolg van het incident en zorg ervoor dat risico’s die verband houden met dit incident worden gemitigeerd. Als er diensten zijn uitbesteed is het noodzakelijk om goede afspraken te maken met de leverancier om incidenten goed op te pakken.

## Kennisgeving

Bepaal welke gegevens mogelijk zijn blootgesteld door het incident en stel de getroffenen in kennis van het feit dat hun gegevens blootgesteld zijn. Als bij Stap 2 ontdekt is dat er een datalek is en dat er een melding gedaan moet worden aan de Autoriteit Persoonsgegevens (AP), dan moet melding bij de AP worden gemaakt en beslist worden of betrokkenen ook geïnformeerd moeten worden. Informeer indien noodzakelijk andere overheidsinstanties, zoals de IBD en/of de politie. Betrek voor deze melding eventueel een jurist van de gemeente (zie: meldingen). Snelheid is ook belangrijk vanuit een PR-oogpunt. Afhankelijk van de aard van het incident kunnen sommige stappen parallel uitgevoerd worden. Let op, het is ook raadzaam om bij de woordvoering over een incident een jurist te betrekken, de aard en inhoud van de communicatie kan gevolgen hebben voor gemeentelijke aansprakelijkheid.

## Rapportage en evaluatie

Identificeer lessen uit het incident en bespreek deze met het team, rapporteer over het incident, de genomen maatregelen en het algemeen verslag, rapporteer indien nodig intern en extern, pas het gevolgde draaiboek aan. Incidenten moeten goed worden opgeschreven, met de oplossing erbij, en bewaard zodat het incidentmanagement proces wordt verbeterd. Er kan lering worden getrokken uit het overzicht met het aantal incidenten en het type incidenten en hier kan vervolgens op worden geacteerd. Belangrijke incidenten moeten daarnaast ook gemeld worden aan de IBD en daarvoor moet een speciale contactpersoon (VCIB) aangewezen worden. Zie hiervoor het aansluitdocument van de IBD. Incidenten melden bij de IBD geeft andere gemeenten ook de mogelijkheid om de kans en de eventuele impact van het incident te verkleinen. Mochten meerdere gemeenten last hebben van hetzelfde incident dan kan de IBD eventueel optreden als contactpersoon richting de leverancier.

## Hoe te gebruiken

Afhankelijk van de aard van het incident en de grootte van het Response team, kan het raadzaam en praktisch zijn om een ​​aantal van de checklist stappen en sub-stappen parallel aan te pakken. Bijvoorbeeld: zodra de oorzaak van een incident wordt bepaald (stap 2.6), remediatie van de oorzaak en het herstel van de functie (stap 3) kan worden gestart, terwijl documentatie activiteiten van stap 2.7 worden aangepakt.

Het is verstandig om de paraatheid van de gemeente op het gebied van ‘veiligheid incident response’ periodiek te oefenen op een manier vergelijkbaar met een noodsituatie planning. Geleerde lessen moeten zo nodig in de checklist, respons procedures, en / of de toewijzing van hulpmiddelen worden opgenomen.

De checklist in bijlage 1 bevat acties die nodig zijn om de meest ernstige veiligheidsincidenten aan te pakken, dat wil zeggen: de blootstelling van persoonlijk identificeerbare informatie beschermd door wetten, standaarden en / of contracten met partijen van buiten de gemeente. Het kan ook effectief worden gebruikt om andere veiligheidsincidenten aan te pakken, bijvoorbeeld: het beschadigen van openbare websites, ongeoorloofde toegang tot vertrouwelijke, maar niet wettelijk beschermde gegevens, of het verlies van vertrouwelijke papieren dossiers.

Gezien de trend naar meer gebruik van derden, met inbegrip van Cloud computing-leveranciers voor het leveren van diensten die gebruik maken van verzamelen, opslaan en/of verwerken van gemeentelijke gegevens, dienen de gemeenten rekening te houden met de gedeelde verantwoordelijkheid voor de incident response. Deze zijn vaak noodzakelijk door dergelijke overeenkomsten. Deze checklist biedt stappen die moeten gebeuren, ongeacht de locatie van een mogelijke inbreuk op de gegevensbeveiliging. Wie de verantwoordelijkheid moet nemen voor elk van deze stappen als een derde partij betrokken is, zal variëren afhankelijk van de aard van de externe dienst, evenals de beveiligings-gerelateerde termen van het contract tussen de gemeente en die partij.

# Aandachtspunten

Welke aspecten komen nog meer bij het incidentmanagement proces kijken? Hieronder staan enkele aspecten die belangrijk zijn voor het incidentmanagement proces.

## Logging

Bij het onderzoek naar mogelijke incidenten wordt veelvuldig gebruik gemaakt van de controle op logging uit systemen, netwerkapparatuur en programma’s. Logbronnen worden gebruikt door een monitoring en response[[1]](#footnote-1) dienst die detecteert of er kwetsbaarheden of incidenten hebben plaatsgevonden. Los van de detectie, wordt logging ook veelvuldig achteraf gebruikt bij het reconstrueren van een incident of om te ontdekken welke systemen nog meer geraakt waren. Logs moeten bewaard worden volgens vaste regels en kennen per soort logging een bewaartermijn waarvan afgeweken kan worden (verlenging) als er een vermoeden is van een incident. Als logging op de juiste wijze bewaard en behandeld wordt, kan logging ook dienen als bewijsmateriaal voor de wet. Let hierbij wel op dat logging persoonsgerelateerde of privacygevoelige informatie kan bevatten, en dat logging zodanig bewaard moet worden dat deze niet zomaar kan worden ingezien of worden gewijzigd. Zie hiervoor de ‘Aanwijzing Logging’ van de IBD . Voor de controle op logging is een voorbeeld cheat sheet te vinden op: <http://www.securitywarriorconsulting.com/security-incident-log-review-checklist.docx>

## Personeel

Het incidentmanagement proces moet een eigenaar hebben en binnen het proces moet een vast aanspreekpunt zijn die eventueel ook zorgdraagt voor de externe communicatie. Het melden van incidenten is een taak van iedereen. De beoordeling van de logging maar ook van gemelde incidenten behoort door een speciaal aangewezen functionaris te gebeuren afhankelijk van waarover de logging of de incidentmelding gaat. In ieder geval moet altijd de servicedesk geïnformeerd worden. Onrechtmatigheden van een bepaalde categorie[[2]](#footnote-2) moeten gemeld worden aan de Chief Information Security Officer (CISO). Bij een escalatie of een noodsituatie moet altijd rekening gehouden worden met woordvoering waarbij de IBD advies kan geven. Al het personeel dat betrokken is bij het incident proces moet op de hoogte zijn van de procedures en de telefonische bereikbaarheid van belangrijke contactpersonen en teamleden. Per soort incident kan het team een wisselende samenstelling hebben.

## Voorbereiding

Rond incidenten kunnen voorbereidingen getroffen en geoefend worden. Voor incidenten met een mogelijke hoge impact is het wenselijk om dat regelmatig te doen. Voor incidenten met hoge impact kunnen zogenaamde cheat sheets [[3]](#footnote-3) of operational incident best practices dan wel standaard operationele digitale incident procedures gemaakt worden. Binnen de wereld van Computer Emergency Response zijn al veel cheat sheets ontwikkeld en deze zijn onder andere te vinden op: <https://cert.societegenerale.com/en/publications.html>. In deze sheets is steeds weer een bepaalde aanpak te herkennen die zeer goed toepasbaar is voor het ontwikkelen van eigen sheets.

In de voorbereiding is het ook belangrijk om iedereen die betrokken zal zijn bij het proces te informeren. Zorg voor overzichten met namen/functies en telefoonlijsten die ook offline beschikbaar zijn. Denk na over communicatie wanneer bijvoorbeeld het totale ICT-infrastructuur (óók VOIP) uitgevallen is of mobiele netwerken overbelast zijn vanwege grote drukte (bij calamiteiten).

## Gouden uur

Het ‘gouden uur’ is het eerste uur na de ontdekking van het incident. Het is essentieel om het incident in te perken maar ook geen informatie verloren te laten gaan die nodig is voor het onderzoek of het onderzoek achteraf. In het geval van bijvoorbeeld een computerinbraak, het wissen van een schijf en de diefstal van data, kan het nodig zijn om een digitaal forensisch expert in te huren[[4]](#footnote-4). Deze kan alleen maar onderzoek doen als er zorgvuldig met bewijsmateriaal omgesprongen wordt. De handelingen uitgevoerd in het eerste uur zijn essentieel voor het welslagen van de reactie, maar ook op de bewijsvoering.

## Gouden tips

1. Vraag bij twijfel advies van een digitaal forensisch expert of bel de Helpdesk van de IBD: 070-3738011.
2. Maak uw standaard procedures.
3. Zorg voor volledig inzicht in de juridische consequenties van het incident en uw betrokkenheid. Ga nooit verder dan uw expertise zal toestaan.
4. Denk verder dan het apparaat in kwestie en let ook op de papieren documentatie, die in het kantoor ligt en mogelijk ook moet worden beschermd om als mogelijk bewijs te dienen.
5. Documenteer nauwkeurig de uitgevoerde acties, deze moeten ook datum en tijd bevatten en gebruik genummerde pagina’s.
6. Vergeet niet om bij het onderzoek de apparatuur te isoleren vanuit elke netwerkverbinding (Bluetooth, bedraad of draadloos).
7. Schakel nooit een apparaat aan als het uit staat.
8. Als een apparaat is ingeschakeld en het lijkt zo te zijn dat dit actief bezig is met het verwijderen van gegevens of onder externe controle is, dan is het te overwegen het apparaat uit te schakelen door het snoer of de batterij weg te nemen. LET OP: niet uitzetten met de aan/uit knop, dan verdwijnen er mogelijk sporen. Win, indien mogelijk, deskundig advies in alvorens iets te doen.
9. Maak desnoods foto’s van externe aansluitingen aan het apparaat, zoals printers of USB-drives en van scherm activiteiten die u kunt zien.

# Incident Prioritering Leidraad

De Incident Prioritering Leidraad beschrijft de regels voor het toekennen van prioriteiten aan incidenten, met inbegrip van de definitie van wat een belangrijk incident is. De incident prioritering wordt herleid uit een tweetal factoren: urgentie en impact. Het toewijzen van de juiste prioriteit aan een incident is essentieel voor het activeren van de geschikte incident maatregelen.

**De prioriteit van een incident wordt meestal bepaald door de beoordeling van de impact en urgentie, waarbij:**

* Urgentie de maat is voor hoe snel de oplossing van het incident vereist is.
* Impact de maat is voor de omvang van het incident en van de mogelijke schade als gevolg van het incident voordat het kan worden opgelost.

## Incident urgentie (categorieën)

In deze paragraaf worden urgentie categorieën verder uitgewerkt. **LET OP: de tabel bevat slechts voorbeelden**.

Om de urgentie van een incident te bepalen, kiest u altijd uit de hoogste waarde van de desbetreffende categorie:

|  |  |
| --- | --- |
| **Categorie Urgentie** | **Omschrijving** |
| **Hoog (H)** | * De schade veroorzaakt door het incident neemt snel toe. * Werk dat moet worden hersteld door personeel is zeer arbeidsintensief. * Een groot incident kan worden voorkomen door bij een klein incident onmiddellijk te handelen. * Het incident leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen voor de bescherming van persoonsgegevens |
| **Medium (M)** | * De schade veroorzaakt door het incident neemt in de tijd aanzienlijk toe. * Er gaat werk verloren, maar dit is relatief snel te herstellen. |
| **Laag (L)** | * De schade veroorzaakt door het incident neemt in de tijd maar weinig toe. * Het werk dat blijft liggen is niet tijdsintensief. |

*Tabel 1: Voorbeelden incident urgentie*

## Incident impact (categorieën)

In deze paragraaf worden de impact categorieën uitgewerkt, de tabel is slechts een voorbeeld.

Om de impact van het incident vast te stellen, kiest u de hoogste desbetreffende categorie:

|  |  |
| --- | --- |
| **Categorie Impact** | **Omschrijving** |
| **Hoog (H)** | * Relatief veel personeel is geraakt door het incident en/of kan zijn/haar werk niet meer doen. Meerdere afdelingen zijn geraakt, de publieksbalie moet gesloten worden. * Inwoners van een gemeente zijn geraakt en/of lijden schade, op welke wijze dan ook, als gevolg van het incident. Persoonsgegevens zijn gecompromitteerd. * De financiële impact van het incident is (bijvoorbeeld) hoger dan €10.000,-. * Het incident leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Bij de beoordeling van de impact van het datalek zijn van belang: * de aard en de omvang van het datalek * de aard van de gelekte persoonsgegevens * de mate waarin technische beschermingsmaatregelen zijn getroffen * de gevolgen voor de persoonlijke levenssfeer van de getroffen personen * Er is reputatieschade, de krant wordt gehaald. * Er zijn lichamelijk gewonden. |
| **Medium (M)** | * Enig personeel is geraakt door het incident en/of kan zijn/haar werk niet meer doen, bijvoorbeeld een afdeling. * Enkele inwoners van een gemeente zijn geraakt en/of lijden schade, op welke wijze dan ook, als gevolg van het incident. Persoonsgegevens zijn gecompromitteerd. * De financiële impact van het incident is (bijvoorbeeld) hoger dan €1.000,- en lager dan €10.000,-. * Er is kans op reputatieschade. |
| **Laag (L)** | * Enkele personeelsleden zijn geraakt door het incident en/of kunnen niet meer hun werk doen. * Enkele inwoners van een gemeente zijn geraakt en/of lijden schade, maar dit is zeer minimaal. Persoonsgegevens zijn gecompromitteerd. * De financiële impact van het incident is (bijvoorbeeld) lager dan €1.000,- * Er is geen kans op reputatieschade. |

*Tabel 2: Voorbeelden incident impact*

## Incident Prioriteringsklassen

De Incident Prioriteit wordt verkregen door urgentie en impact tegen elkaar af te zetten.

**Incident Prioriteiten Matrix**

Als er klassen zijn gedefinieerd om urgentie en impact in te schalen, dan kan een Incident Prioriteit Matrix gebruikt worden om prioriteringsklassen te herleiden. In het onderstaande voorbeeld zijn de klassen uitgewerkt met een code en kleuren.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **Impact** | | |
| Hoog | Midden | Laag |
| **Urgentie** | Hoog | 1 | 2 | 3 |
| Midden | 2 | 3 | 4 |
| Laag | 3 | 4 | 5 |

*Tabel 3: Incident prioriteringklassen*

|  |  |  |  |
| --- | --- | --- | --- |
| **Code/kleur** | **Omschrijving** | **Reactietijd** | **Oplossingstijd** |
| **1** | Kritiek | Onmiddellijk | 1 uur |
| **2** | Hoog | 10 minuten | 4 uur |
| **3** | Medium | 1 uur | 8 uur |
| **4** | Laag | 4 uur | 24 uur |
| **5** | Zeer laag | 1 dag | 1 week |

*Tabel 4: Incidenten prioriteiten matrix*

### Omstandigheden die het noodzakelijk maken dat een incident behandeld wordt als een groot incident

*Grote incidenten hebben een ander soort Incident managementteam nodig en maken gebruik van een gescheiden proces dat speciaal is ingericht voor het behandelen van grote incidenten.*

### Indicatoren

Niettegenstaande de bovenstaande prioritering, is het vaak nodig om aanvullende, gemakkelijk te begrijpen, indicatoren vast te stellen voor het identificeren van grote incidenten (zie ook de toelichting hieronder op het identificeren van grote incidenten ongevallen). Voorbeelden van dergelijke indicatoren zijn:

1. Bepaalde (groepen van) bedrijfskritische diensten, toepassingen of onderdelen van de infrastructuur zijn niet beschikbaar en de geschatte tijd voor herstel is onbekend of extreem lang (nader te specificeren diensten, toepassingen of onderdelen van de infrastructuur).
2. Bepaalde (groepen van) vitale bedrijfsfuncties (bedrijfskritische processen) worden beïnvloed en de geschatte tijd voor het herstellen van deze processen tot volledige operationele status is onbekend of extreem lang (specificeren bedrijfskritische processen).

### Het identificeren van kritische incidenten

Hoewel servicedeskmedewerkers door ervaring vaak een goed idee hebben ontwikkeld over wat een kritisch incident is, blijft het moeilijk om een eenduidige definitie van dit begrip te geven. Daarom is het waarschijnlijk beter om de definitie zo ruim mogelijk te interpreteren.

Een kritisch incident wordt meestal getypeerd door zijn impact, vooral de impact op gebruikers speelt hierbij een belangrijke rol. Enkele voorbeelden:

* Een deel van de datacommunicatie van en naar de gemeente ligt plat door een storing in het netwerk.
* Een belangrijke database blijkt corrupt te zijn.
* Meerdere servers worden geïnfecteerd door een ‘worm’.
* Persoonsgegevens en vertrouwelijke informatie van burgers worden per ongeluk op een publiek toegankelijk forum geplaatst.

Bedenk ook dat alle rampen zoals onderkend in een continuïteitsplan, kritische incidenten zijn en ook dat kleinere incidenten door een niet afdoende afhandeling, zich tot kritische incidenten kunnen ontwikkelen.

### Belangrijkste eigenschappen van kritische incidenten

Enkele belangrijke gevolgen van kritische incidenten zijn:

* Een groot aantal gebruikers/klanten of enkele belangrijke gebruikers/klanten kunnen mogelijk geen gebruik maken van diensten of systemen.
* Een aantal systemen die belangrijk zijn voor de uitvoering van rampenbestrijding en crisisbeheersing vallen uit of zijn niet benaderbaar.
* De kosten (inclusief gevolgschade) voor gebruikers/klanten of voor de gemeente zijn aanzienlijk of kunnen aanzienlijk worden.
* Het incident leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. De gemeente zou reputatieschade kunnen oplopen.

En:

* De tijd en moeite die nodig zijn om het incident op te lossen zijn waarschijnlijk groot en het is zeer waarschijnlijk dat afspraken die zijn vastgelegd in de SLA niet kunnen worden nagekomen.

Een kritisch incident kan ook worden omschreven als een ‘majeur incident’ of een ‘incident met hoge prioriteit’.

# Bijlage 1: Incidentmanagement en response beleid stappenplan en sjabloon

**Incidentmanagement en response beleid stappenplan**

Incident # \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Datum ontdekking: \_\_\_\_\_\_\_\_\_\_\_\_ Datum gerapporteerd aan de CISO en het management: \_\_\_\_\_\_\_\_\_\_\_\_

Datum informatieverstrekking getroffenen: \_\_\_\_\_\_\_\_\_\_

*(Dit zou binnen een week na de ontdekking moeten zijn)*

*Incident met persoonsgegevens: JA / NEE*

**Type en scope van de gecompromitteerde data:**

**Incident team samenstelling:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| STAP 1: Identificatie  Controleer of een incident daadwerkelijk heeft plaatsgevonden. Deze activiteit omvat normaliter de systeembeheerder en eindgebruiker, maar kan ook het gevolg zijn van proactieve detectie van incidenten door de ICT-beveiliging of het systeembeheer. Indien wordt vastgesteld dat het inderdaad een incident is, dan moeten de betreffende instanties gewaarschuwd worden. | | | | |
| *Gedaan* | ***Taak*** | ***Eigenaar*** | | *Notities* |
|  | 1. Onmiddellijk blootstelling beperken:  * Als een elektronisch apparaat is gecompromitteerd:   + Niet gebruiken (niet inloggen) of wijzigen van het apparaat   + Zet het apparaat niet uit   + Haal de netwerkverbindingen er af, maar NIET de voedingskabel * Noteer hoe het incident werd ontdekt en welke acties er tot nu toe genomen zijn. Geef een zo specifiek mogelijk antwoord, inclusief data, tijden, en welke apparaten gecompromitteerd zijn, applicaties, websites, et cetera. | Afdeling | |  |
|  | 1. Waarschuw onmiddellijk de servicedesk (incidentmanager) en de CISO   *Handleiding: Voeg namen en telefoonnummers, e-mailadressen of indien mogelijk de link naar een online meldingsformulier toe.* | Afdeling | |  |
|  | 1. Indien het incident over elektronische apparaten gaat of als er media gestolen of verloren is, dan ook aangifte doen bij de politie.   *Handleiding: Deze stap alleen uitvoeren na overleg en op advies van de CISO of ICT- security afdeling.* | Afdeling | |  |
|  | 1. Voer een voorlopige beoordeling uit van het type en de scope van het incident en de omvang van de blootstelling. Als er potentieel gevoelige informatie blootgesteld is dan moet het management geïnformeerd worden en deze moet tijdens het verloop van het incident op de hoogte gehouden worden:   *Voorbeelden:*   1. *CIO* 2. *Gemeentesecretaris* 3. *Voorlichting* 4. *IBD* 5. *B&W*     * Start met een logboek waarin gedurende het incident alle activiteiten op datum en tijd kunnen worden vastgelegd.    * Indien het incident ook het lekken van persoonsgegevens betreft, leg dit dan nu vast. | CISO of incidentmanager of -management | |  |
|  | 1. Indien er sprake is van criminele activiteiten in verband met het incident moet bepaald worden of de politie mogelijk het onderzoek moet overnemen. Als dat gebeurt zal dit het vervolg van dit schema beïnvloeden. |  | |  |
| *STAP 2: Schade indamming en beoordeling van de blootstelling*  *Wijs een Incident response-teamleider aan en stel een bij het incident passend, ‘Incident response team’ samen. Dit team is belast met het beperken van verdere schade als gevolg van het incident. Start een grondige beoordeling van de aard en omvang van het incident en stel vast wat de schade is. Stel bewijsmateriaal veilig.* | | | | |
|  | 1. Stel het Incident response team samen   *Handleiding: Zorg ervoor dat de vertegenwoordiger van de organisatie-eenheid waar het incident zich voordeed, deelneemt en dat deze persoon hoog genoeg in de organisatie zit om de nodige beslissingen te nemen.* | Incidentmanager of -management | |  |
|  | 1. Beoordeling Incident response proces en de verantwoordelijkheden met het Incident response team  * Verstrek ieder teamlid de huidige incidentmanagement Checklist. * Bespreek de communicatiestrategie. * Bespreek het belang van het goed in een tijdlijn documenteren en het voorkomen van het verloren raken van onderzoeksgegevens.   *Handleiding: Aangaande het bespreken van de regels van de communicatie met het team in deze fase, is het vooral belangrijk om de nauwkeurigheid van de feiten te waarborgen tussen teamleden onderling en tussen het team en de juiste ambtenaren.*  *Voorbeelden:*   1. *Teamleden mogen niet praten met anderen buiten het team over het incident totdat er daarvoor toestemming is gegeven door het management of de CISO.* 2. *Alle documentatie die door het team geschreven wordt moet op feiten gebaseerd zijn omdat het mogelijk in een strafrechtelijk onderzoek gebruikt kan worden.* 3. *Er is dagelijks overleg tussen de teamleden.* 4. *Het team moet bijhouden hoeveel tijd er besteed wordt en waaraan.* | De manager van het Incident response team | |  |
|  | 1. Verzamelen en veiligstellen van bewijsmateriaal   *Handleiding: Verzamel fysiek en digitaal bewijs die tezamen een duidelijke, gedetailleerde beschrijving geven van hoe de data gecompromitteerd kon worden.*  *Voorbeelden:*   1. *Images van de harddisk(en)* 2. *Netwerkverkeersgegevens van en naar de gecompromitteerde apparatuur* 3. *Werkplek applicatie logs* 4. *Toegangslogs* 5. *Foto’s van de omgeving waar het incident plaatsvindt* | Incident response team | |  |
|  | 1. Zorg voor, en onderhoud, al het bewijsmateriaal en houd bij waar het zich bevindt en wie er toegang toe heeft.   *Handleiding: Maak een inventarisatielijst van alle bewijsmateriaal en houdt bij wie, wanneer, wat gedaan heeft met het bewijsmateriaal.*  *Voorbeelden:*   1. *Beschrijf wat exact het bewijsmateriaal is.* 2. *Leg vast wie erbij moest en waarom.* 3. *Leg vast waar en hoe het bewijsmateriaal opgeslagen is.* 4. *Als apparatuur verplaatst moet worden zorg dan dat de ontvanger getekend heeft voor ontvangst en dat dit bewijs wordt toegevoegd aan de verzameling. Zorg dat de ontvanger weet welke verantwoordelijkheden er zijn.* | Incident response team | |  |
|  | 1. Neem maatregelen om de scope en de impact van het incident in te perken.   *Voorbeelden:*   1. *Indien het incident betrekking heeft op gevoelige gegevens die onjuist geplaatst zijn op publiek toegankelijke websites, verwijder dan de actieve en opgeslagen inhoud en verzoek om verwijdering van de gecachte[[5]](#footnote-5) of in proxy opgeslagen webpagina(‘s), die geïndexeerd zijn door zoekmachine bedrijven en andere Internet-archief bedrijven, zoals bijvoorbeeld de Wayback Machine.* 2. *Verander mogelijk gecompromitteerde wachtwoorden.* 3. *Staak de exploitatie van een gecompromitteerde applicatie of server.* | Incident response team | |  |
|  | 1. Voer forensisch onderzoek uit en leg dit vast:    1. Analyseer bewijsmateriaal    2. Voer een reconstructie uit van het incident    3. Zorg voor gedetailleerde documentatie   *Handleiding: Bewaar origineel bewijsmateriaal en werk alleen op een kopie van de data. Zorg voor minimale verstoring van de bedrijfsvoering, zorg voor herleidbare en herhaalbare resultaten.* | Incident response team | |  |
|  | 1. Maak de definitieve schatting af, en de documentatie over soort en afbakening van de blootgestelde data, evenals de beschikbaarheid en het soort van contactinformatie van de betrokken personen. | Incident response team | |  |
|  | Geef mogelijk een voorwaarschuwing aan de Autoriteit Persoonsgegevens.  Handleiding:  Als er een datalek is en deze valt onder de meldplicht datalekken van de AVG, dan moet er op basis van de beschikbare gegevens een voormelding gedaan worden bij de Autoriteit Persoonsgegevens. | CISO of incidentmanager of –management of Privacy Functionaris | |  |
| STAP 3: Remediatie en herstel  Neem maatregelen om de oorzaak van het incident te blokkeren of te verwijderen, verminder de impact door verdere blootstelling van de gevoelige gegevens te voorkomen, maak een start om de bedrijfsprocessen te herstarten als deze gestopt waren als gevolg van het incident en zorg ervoor dat risico’s die verband houden met dit incident worden gemitigeerd. | | | | |
|  | 1. Ga terug naar stap 2.4 en zoek naar aanvullende manieren om de blootstelling te beperken.     *Voorbeelden:*   1. *Run periodiek web-queries om u er van te verzekeren dat de data niet verder is verspreid of gecached.* 2. *Beoordeel de inventarisatie van getroffen hardware en systemen en wijzig verder waar nodig de wachtwoorden die mogelijk gecorrumpeerd zijn.* 3. *Stop eventueel gecorrumpeerde diensten of applicaties en zorg voor work-arounds* | Incident response team | |  |
|  | 1. Verwijder of mitigeer kwetsbaarheden van systemen, beoordeel toegangsrechten en remediatie risico’s voor gevoelige dataopslag     *Voorbeelden:*   1. *Run vulnerability scans op getroffen systemen;* 2. *Beoordeel en bepaal waar de data zich bevindt en wijzig dit indien nodig om een hogere beschermingsgraad te verzekeren.* 3. *Beperk de toegang tot systemen tot uitsluitend degenen die toegang nodig hebben.* 4. *Gebruik software tools om gevoelige data te vinden, te verwijderen en te beschermen, bijvoorbeeld: Identity Finder.* | Incident response team | |  |
|  | 1. Als het onderzoek naar de bewijslast op de gecompromitteerde systemen klaar is kunnen ze weer in gebruik genomen worden. |  | |  |
| STAP 4: Kennisgeving  Bepaal welke gegevens mogelijk zijn blootgesteld door het incident en stel de getroffenen in kennis van het feit dat hun gegevens blootgesteld zijn. Snelheid is geboden indien er persoonsgegevens verloren zijn gegaan of bekend geworden zijn aan niet rechthebbenden. Informeer indien noodzakelijk andere overheidsinstanties, zoals de IBD en/of de politie. Bij sommige incidenten is het wettelijk verplicht een melding te doen naar andere instanties. Snelheid is ook belangrijk vanuit een PR-oogpunt. Afhankelijk van de aard van het incident kunnen sommige stappen parallel uitgevoerd worden. | | | | |
|  | 1. Neem beslissingen op basis van de bevindingen van het Incident response team  * Geeft de mate van risico blootstelling de noodzaak tot het informeren van getroffenen?[[6]](#footnote-6) * Zo ja, * Indien van toepassing, is het de taak van rechtshandhaving om de betrokken partijen te infomeren? * Wie gaat het schrijven uitgeven? * Wie zal zich bezighouden met het beantwoorden van telefoon en e-mail op vragen van de betrokken personen? Rechtvaardigt het verwachte volume het opzetten of inzetten van een call center? * Is het noodzakelijk om een officieel persbericht te plaatsen op de website van de gemeente? * Als er geen kans is geweest op blootstelling van informatie aan buitenstaanders, dan kan eventueel meteen doorgegaan worden naar stap 5.  1. Indien het een incident betreft met persoonsgegevens waarbij een aanzienlijke kans bestaat op ernstige nadelige gevolgen voor de betrokkene dient de toezichthouder onverwijld in kennis gesteld te worden.[[7]](#footnote-7)   *Handleiding:*   1. *Degenen die verantwoordelijk zijn voor het nemen van deze beslissingen zal variëren van gemeente tot gemeente, maar meestal is een deel van de ambtenaren geïnformeerd in Sub-stap 1.4. Beslissingen die genomen moeten worden, dienen in overeenstemming te zijn met eerdere beslissingen, tenzij eventuele afwijkingen volledig gerechtvaardigd zijn. Uiteraard moeten voor alle beslissingen de respectievelijke wetten, regelgeving en contractuele verplichtingen worden gevolgd.* 2. *Er moet een geschikt communicatiemiddel gekozen worden, passend bij het incident, de hoeveelheid te informeren personen, de mate waarin risico gelopen is en/of informatie gecompromitteerd is.* 3. *Er dient juridisch advies ingewonnen te worden over de positie en aansprakelijkheid van de gemeente bij bepaalde communicatie.* | Management |  | |
|  | 1. Verzamel de naam en adresgegevens van de getroffenen   *Handleiding: Dit kan een moeilijk proces zijn als er mensen geraakt zijn waarvan de gemeente geen NAW-gegevens heeft.*  *Zorg ervoor dat de verzamelde data veilig wordt behandeld, verstuurd en opgeslagen en als de data niet langer benodigd is moet deze worden vernietigd.* | Afdeling, geadviseerd door de CISO of door het Incident response team |  | |
|  | 1. Zet telefoon en e-mail ondersteuning op in geval van vragen:    * Stel een team samen.    * Zorg voor voldoende infrastructuur, beoordeel of de lijn en e-mail capaciteit voldoende is.    * Kies een geschikt telefoonnummer om te gebruiken.    * Kies een geschikt e-mailadres om te gebruiken.    * Bedenk van te voren de reacties op de verwachte vragen.    * Train het team. | Afdeling, geadviseerd door de CISO of door het Incident response team |  | |
|  | 1. Als in stap 4.1 een website gekozen is om te communiceren:    * Verzin een URL en website locatie.    * Voorkom toegang totdat de website live mag gaan.    * Bereid de inhoud voor.   *Handleiding:*   1. *Websites worden vooral gemaakt als het aantal getroffenen te groot is of omdat niet alle mensen bekend zijn.* 2. *De website content moet goedgekeurd worden.* | Afdeling, geadviseerd door de CISO of door het Incident response team |  | |
|  | 1. Voorbereiding schriftelijke informatieverstrekking aan getroffenen:  * Bedenk het onderwerp en de huisstijl. * Schrijf een concept tekst.   *Handleiding:*  *De inhoud van de brief moet zijn goedgekeurd door het management en door voorlichting.* | Afdeling, geadviseerd door de CISO of door het Incident response team |  | |
|  | 1. Als er een noodzaak of een verplichting is, informeer de politie en doe aangifte. | Management |  | |
|  | 1. Informeer de Informatie Beveiligingsdienst (IBD) | CISO of ACIB/VCIB  na afstemming met het management |  | |
|  | 1. Doe de definitieve melding aan de Autoriteit Persoonsgegevens (AP) als er bij Stap 2.8 een voor melding gedaan is. Doe een gemotiveerde melding aan de AP als er bij Stap 2.8 geen voormelding gedaan is en er toch meldplichtige persoonsgegevens gelekt zijn. (Gemotiveerd, omdat als bij een AP melding meer dan 72 uur vergaan zijn sinds de ontdekking van het datalek, je moet uitleggen waarom je pas na 72 uur een melding doet.) | Management of Privacy Functionaris |  | |
|  | 1. Informeer derde partijen zoals service providers als hiermee het risico van identiteitsdiefstal verkleind kan worden of als dat is vastgelegd in het respectievelijke contract. | Afdeling |  | |
|  | 1. Als er bankgegevens blootgesteld zijn aan niet rechthebbenden, informeer dan de bank of creditcard firma’s. | Controller |  | |
|  | 1. Coördineer de gelijktijdige communicatie-acties zodat de verschillende informatiestromen gelijktijdig plaatsvinden. | Afdeling, Voorlichting |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| STAP 5: Rapportage en evaluatie  Identificeer lessen uit het incident en bespreek deze met het team, rapporteer over het incident, de genomen maatregelen en het algemeen verslag, rapporteer indien nodig intern en extern, pas het gevolgde draaiboek aan. | | | |
|  | 1. Verzamel alle tijdschrijfregels van het personeel dat heeft meegewerkt aan de Incident response-actie. De totale kosten kunnen mogelijk van belang zijn indien er een rechtszaak komt tegen een verdachte, omdat deze dan verhaald kunnen worden. | Iedereen die tijd geschreven heeft rapporteert aan het management |  |
|  | 1. Plan een vergadering ongeveer 2 tot 6 weken na het incident om een evaluatie uit te voeren over de aanpak van het incident. | Incident response team |  |
|  | 1. Onderzoek oplossingen om herhaling te voorkomen.    * Indien nodig rapporteer hierover aan het management.   *Te beantwoorden vragen:*   1. *Waarom was de data opgeslagen op een verkeerde plaats of niet veilige plaats?* 2. *Wat hadden we meer kunnen doen om de inbraak te voorkomen?* 3. *Neemt de afdeling voldoende maatregelen om herhaling te voorkomen?* | CISO |  |
|  | 1. Plan oplossingsprojecten om de geleerde lessen effectief in te bedden in de organisatie. | Afdeling |  |
|  | 1. Sla alle Incident en response informatie veilig op, inclusief gesprekverslagen, aantekeningen en incident artefacten. In overeenstemming met wetgeving en intern beleid zal op enig moment (een deel van) de opgeslagen informatie vernietigd moeten worden.   Indien het een inbreuk betreft van de bescherming van persoonsgegevens[[8]](#footnote-8) moet altijd een overzicht hiervan worden bijgehouden. | CISO |  |

# Bijlage 2: Incidentenprocedure informatiebeveiliging

### Melding van een informatiebeveiligingsincident

Elke medewerker dient alert te zijn op bedreigingen met betrekking tot informatiebeveiliging en is verplicht om alle incidenten die hij/zij ontdekt of vermoedt te melden aan de helpdesk.In gevalhet vertrouwelijke zaken of personen betreft, moet de melding ook rechtstreeks aan de CISO gedaan worden.

### Toewijzen en escaleren van een informatiebeveiligingsincident

Hieronder staat een lijst (twee tabellen) met mogelijke incidenten m.b.t. informatiebeveiliging. Deze lijst is niet uitputtend en zal dit ook nooit kunnen zijn: er zullen zich steeds nieuwe soorten beveiligingsincidenten voordoen. De lijst ondersteunt de helpdesk bij het herkennen van een beveiligingsincident en bij het inschatten van de impact. Het is aan te bevelen dat bij twijfel de helpdesk contact opneemt met de Security Officer.

In veel gevallen zal de Security Officer niet als primaire behandelaar optreden, immers het technisch verhelpen van een dergelijk incident gebeurt niet door de Security Officer, maar door een technisch specialist. Het incident wordt dan door de helpdesk opgesplitst in deelincidenten, die naar de betrokken behandelaars worden gestuurd.

De Security Officer kan op twee manieren worden ingeschakeld:

1. De Security Officer moet direct een incident met hoge prioriteit oplossen, dan wel coördineren of adviseren. In dit geval neemt de helpdesk direct telefonisch contact op met de Security Officer (of vervanger).
2. De Security Officer moet op de hoogte worden gebracht dat een incident is gebeurd. Indien nodig is het incident ook naar een andere specialist gestuurd ter behandeling. De Security Officer raadpleegt de meldingsdatabase regelmatig (ongeveer 1 keer per week).

Er zijn twee invallers voor de Security Officer, in geval incidenten met hoge prioriteit behandeld moeten worden:

* Hoofd Facilitair Beheer, die ook de fysieke beveiliging in het takenpakket heeft.
* Hoofd afdeling Informatie en Beheer.

Acties Security Officer

* De Security Officer neemt direct maatregelen om bewijsmateriaal en andere gegevens die in dit stadium als relevant worden beschouwd, veilig te stellen.
* De Security Officer bepaalt hoeveel tijd en middelen nodig zijn voor afhandeling van het beveiligingsincident. Aan de hand hiervan en de ernst van het incident bepaalt de Security Officer in overleg met het management of aan het incident prioriteit moet worden gegeven en of een onderzoeksteam samengesteld moet worden.

### Alarmeringsprocedure

Indien de Security Officer inschat dat de ernst van het incident dusdanig is óf acties nodig zijn die de handelingsbevoegdheid van de Security Officer te boven gaan, wordt de directe leidinggevende of de directie ingeschakeld.

# Bijlage 3: Incidenten en meldingsniveau matrix

| **GEBRUIKERS­INCIDENTEN** |  | **NIVEAU VAN MELDING \*)** | | |
| --- | --- | --- | --- | --- |
| **Incidenten categorie** | **Mogelijk incident** | **Helpdesk** | **CISO** | **Directie** |
| 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 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** | **Mogelijk incident** | **Helpdesk** | **CISO** | **Directie** |
| 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 |  |
| Onopzettelijk foutief handelen van gebruikers | Onzorgvuldige omgang met wachtwoorden door gebruikers | X | X |  |
| Opzettelijk foutief handelen van gebruikers | Kraken of omzeilen toegang door medewerkers 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 netwerk verbinding 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 gemeente | X | X | X |

\*) Niveau van Melding:

* Helpdesk: Incidenten die door gebruiker en/of beheerder worden gemeld bij helpdesk.
* CISO: Incidenten die door helpdesk worden gemeld bij de CISO of andere Security Officer.
* Directie: Incidenten die door Security Officer worden gemeld bij directie.

# Bijlage 4: Definities

**Een gebeurtenis of event** is een waarneembare verandering in het normale gedrag van een systeem, omgeving, proces, workflow of persoon.

Er zijn drie basistypen van informatiebeveiligingsgebeurtenissen:

**Normaal** - een normale gebeurtenis heeft geen invloed op cruciale onderdelen van het systeem en zal ook niet eisen dat er extra controles moeten worden uitgevoerd. Normale gebeurtenissen vereisen geen interventie van hoger personeel of het management en er is geen melding van het event vereist.

**Escalatie** - een geëscaleerd event treft kritische productiesysteem of -systemen en vereist dat er maatregelen genomen moeten worden om mogelijke gevolgen in te perken en verdere schade, dan wel uitval, te voorkomen van dat systeem of deze systemen. Geëscaleerde gebeurtenissen vereisen de deelname van hoger personeel en het informeren van belanghebbenden zoals systeemeigenaren, leidinggevenden en het Response team.

**Emergency of noodsituatie** - een noodsituatie is een gebeurtenis die verregaande gevolgen zal hebben voor grote delen van de informatievoorziening en daarmee van de bedrijfsvoering van de gemeente, maar kan ook invloed hebben op de gezondheid of veiligheid van de mensen. Een noodsituatie vereist onmiddellijk handelen, maar niet nadat met zekerheid is vastgesteld wat er precies aan de hand is. Een noodsituatie kan alleen uitgeroepen worden door een incident coördinator na afstemming met het (lijn)management of de directie.

In alle gevallen moeten incidenten opgevolgd worden volgens een Computer Security Incident Response-plan op basis van de incidentmanagement en response checklist. Sommige incidenten kunnen voorspelt worden en dus kan er voor een aantal mogelijke incidenten van te voren een Response-plan gemaakt worden.

**Incident Escalatie Regels**

Een set van regels waarin een hiërarchie voor escalatie Incidenten en triggers die leiden tot escalaties. Triggers zijn meestal gebaseerd op de ernst van incidenten en oplostijden.

**Incidentmanagement Rapport**

Een verslag leveren van Incident-gerelateerde informatie aan de andere management processen.

**Incident Model of cheat sheet**

Een Incident-model bevat de vooraf gedefinieerde stappen die moeten worden genomen voor het omgaan met een bepaald type Incident. Dit is een manier om ervoor te zorgen dat regelmatig voorkomende incidenten daadwerkelijk en efficiënt worden afgehandeld. Zie ook bijvoorbeeld: <http://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901?show=incident-handlers-handbook-33901&cat=incident>

**Incident Prioritering Leidraad**

De Incident Prioritering Leidraad beschrijft de regels voor het toekennen van prioriteiten aan incidenten, met inbegrip van de definitie van wat een Noodsituatie Incident. Omdat incidentmanagement escalatie regels meestal gebaseerd zijn op prioriteiten, is het toewijzen van de juiste prioriteit aan een incident essentieel voor het activeren van passende escalaties. Zie ook: Checklist Incident Prioritering Leidraad.

**Incident Record**

Een verzameling van gegevens met alle details van een incident, het documenteren van de geschiedenis van het incident van registratie tot sluiting. Elke gebeurtenis die mogelijk een risico kan gaan worden in de toekomst, is ook een incident (bijv. het uitvallen van een harde schijf van een reeks gespiegelde drives). Zie ook: Checklist Incident Record

**Incident Status Informatie**

Een bericht met de huidige status van een incident verzonden naar een gebruiker die eerder melding deed. Statusinformatie wordt doorgaans aan gebruikers op verschillende punten tijdens de levenscyclus van een incident.

**Proactieve gebruikersinformatie**

Een mededeling voor gebruikers van bestaande of dreigende incidenten of verstoringen, zelfs als de gebruikers zich nog niet bewust van de onderbrekingen, zodat gebruikers in staat zijn om zich voor te bereiden voor een periode van niet beschikbaarheid of verminderde van de dienst.

**Pers**

Pers woordvoering in verband met informatiebeveiligingsincidenten is een apart specialisme, besef dat goede woordvoering en goede communicatie een incident kunnen ondersteunen, maar ook dat verkeerde woordvoering voor een verdere escalatie kunnen zorgen.

**IBD**

De Informatiebeveiligingsdienst voor Gemeenten, een onderdeel van VNG/KING die gemeenten preventief en structureel ondersteunen bij het opbouwen en onderhouden van bewustzijn als het gaat om informatiebeveiliging.

**Support Aanvraag**

Een verzoek om een incident of probleem te ondersteunen, meestal uitgegeven door de Incident Manager wanneer verdere hulp nodig is van een derde partij zoals de IBD, maar ook het escaleren om daarmee anderen te kunnen waarschuwen.

**Gebruiker FAQ’s**

Zelf Help informatie voor gebruikers van de gemeente, meestal als onderdeel van de ondersteuningspagina's op het intranet.

**Aangifte**

Bij digitale inbraak moet altijd aangifte gedaan worden. Het maakt daarbij niet uit of de bedoeling achter inbraak per ongeluk of kwaadwillend was.

# Bijlage 5: Incidentmanagement en response beleid gemeente <gemeente>

Het incidentmanagement en response beleid van de gemeente geeft richting aan de wijze waarop de gemeente wenst om te gaan met alle incidenten en bijna incidenten op het gebied van informatiebeveiliging. De gemeente onderschrijft het belang van een adequate behandeling van incidenten en de response daarop om daarmee de gevolgen voor de bedrijfsvoering te minimaliseren. Incidenten dienen gestructureerd te worden behandeld en er moeten procedures worden vastgesteld om de reactie op incidenten doeltreffend en ordelijk te laten plaatsvinden. De gemeente wil leren van incidenten, en daarom moeten incidenten geëvalueerd worden. Dit beleid is van toepassing op de iedereen die werkzaam is bij de gemeente.

Iedere medewerker, zowel vast als tijdelijk, intern of extern is **verplicht waar nodig gegevens en informatiesystemen te beschermen** tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

De volgende uitgangspunten zijn vastgesteld voor de gemeente en deze zijn ontleend aan het gemeentelijk informatiebeveiligingsbeleid en de BIO:

1. Informatiebeveiligingsgebeurtenissen en zwakheden die verband houden met informatiesystemen worden zodanig kenbaar gemaakt dat de gemeente tijdig en adequaat corrigerende maatregelen kan nemen. Dit omvat ook het regelmatig beoordelen van loggegevens van informatiesystemen.
2. Informatiebeveiligingsgebeurtenissen moeten zo snel als mogelijk via de leidinggevende of de helpdesk of de CISO gerapporteerd worden.
3. Alle werknemers, ingehuurd personeel en externe gebruikers van gemeentelijke informatiesystemen en diensten moeten alle waargenomen of verdachte zwakke plekken melden volgens de procedure.
4. Informatiebeveiligingsincidenten moeten vastgelegd en beheerd worden en hiervoor zijn procedures gemaakt. Deze procedures moeten bekend zijn bij alle werknemers. In deze procedures moeten de verantwoordelijkheden belegd worden.
5. Informatiebeveiligingsmeldingen moeten periodiek beoordeeld worden met als doel de beheersmaatregelen te verbeteren.
6. Informatiebeveiligingsincidenten kennen soms een vervolgprocedure, daarom moet zoveel als mogelijk bewijsmateriaal verzameld worden in overeenstemming met de voorschriften.
7. Informatiebeveiligingsincidenten moeten geëvalueerd worden zodat de procedures kunnen worden bijgesteld en beheersmaatregelen kunnen worden verbeterd.

Aldus vastgesteld door burgemeester en wethouders van *[gemeente]* op *[datum],*

[Naam. Functie] [Naam. Functie]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Icon

Description automatically generated

Nassaulaan 12

2514 JS Den Haag

CERT: 070 204 55 11 (9:00 – 17:00 ma – vr)

CERT 24x7: Piketnummer (instructies via voicemail)

[info@IBDGemeenten.nl](mailto:info@IBDGemeenten.nl) / [incident@IBDGemeenten.nl](mailto:incident@IBDGemeenten.nl)

Kijk voor meer informatie op:

www.informatiebeveiligingsdienst.nl

1. Handreiking Monitoring en Response Starten met & handreiking Monitoring en Response uitbreiden [↑](#footnote-ref-1)
2. Zie Bijlage: Incidentmanagement en response stappenplan en sjabloon [↑](#footnote-ref-2)
3. Cheat sheets worden binnen het ICT-domein regelmatig gebruikt bij systeemontwikkeling en systeembeheer. [↑](#footnote-ref-3)
4. Zie hiervoor de [handreiking Digitaal Forensisch Onderzoek](https://www.informatiebeveiligingsdienst.nl/product/digitaal-forensisch-onderzoek/) [↑](#footnote-ref-4)
5. Een cache (spreek uit: kesj of kasj, van het Franse werkwoord 'cacher', verbergen) is een opslagplaats waarin gegevens tijdelijk worden opgeslagen om sneller toegang tot deze data mogelijk te maken. Essentieel van een cache is ook dat het transparant is in die zin dat het bij het ophalen van data niet zichtbaar is of het bij de originele bron wordt opgehaald of uit de cache wordt gehaald, afgezien de korte toegangstijd. [↑](#footnote-ref-5)
6. Bijvoorbeeld bij niet versleutelde persoonsgegevens die gelekt zijn. [↑](#footnote-ref-6)
7. Art 43a Wet meldplicht datalekken: De verantwoordelijke stelt het College onverwijld in kennis van een inbreuk op de beveiliging, bedoeld in artikel 13, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. [↑](#footnote-ref-7)
8. [Zie AVG 33a lid 5.](https://wetten.overheid.nl/jci1.3:c:BWBR0040940&hoofdstuk=3&paragraaf=3.2&artikel=33&z=2018-05-25&g=2018-05-25) . [↑](#footnote-ref-8)