nationale ombudsman

Vertrouwelijk

Incident Management

Document classificatie

Vertrouwelijk

Versiebeheer

Versienummer	1.0 DEFINITIEF
Opgesteld door	Matthijs Kerkvliet
Datum eerste versie	18 september 2020
Laatst bijgewerkt	17 september 2021
Bron van het document	Informatiebeveiligingsdienst (IBD)

Geschiedenis wijzigingen

Versienr.	Datum	Auteur	wijzigingen
0.2	25-9-2020	Matthijs Kerkvliet	Omgeschreven naar No
0.3	07-10-2020	Martijn de Bruin	
0.4	8-10-2020	Andrik Eker	
0.5	23-10-2020	Matthijs Kerkvliet	Procedure melding datalek buiten incidentmanagement
0.6	05-11-2020	Martijn de Bruin Andrik Eker	

0.7	13-11-2020	Matthijs Kerkvliet	
0.8	29-01-2021	Matthijs Kerkvliet	Versie na eerste evaluatie
0.9	23-06-2021	Matthijs Kerkvliet	Versie na workshop werkinstructie incidentmanagement
0.9.2	23-07-2021	Rion Rijker	Review op basis van gemaakte aanpassingen.
0.9.3	30-7-2021	Rion Rijker	Update op basis van gezamenlijke review
0.95	3-08-2021	Matthijs Kerkvliet	Gegevens in bijlage 3 geupdate. Nog finaliseren voor versie BVO
1.0	17-9-2021	Matthijs Kerkvliet	Versie vastgesteld in BVO

Inhoud

1 Inleiding

Incidentmanagement 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. Het primaire doel is de ontwikkeling van een goed begrepen en voorspelbare reactie op schadelijke gebeurtenissen in de meest brede zin van het woord. De wijze waarop een datalek wordt gemeld en vervolgens afgehandeld valt buiten de scope van deze beschrijving, tenzij tijdens de behandeling van een incident wordt vastgesteld dat het incident ook heeft geleid tot een datalek. In dat geval wordt de FG hiervan op de hoogte gesteld en zal de FG het datalek verder in behandeling nemen.

De Nationale ombudsman moet zich bewust zijn van de verantwoordelijkheden als het gaat om de bescherming van informatie ten behoeve van de burgers en (Rijks)overheid. Deze verantwoordelijkheid strekt zich uit tot het hebben van een draaiboek voor 'wat te doen, als er iets misgaat'.

1.1 Beschikbaarheid, Integriteit en Vertrouwelijkheid

Incidentmanagement is een belangrijk onderdeel van informatiebeveiliging. Niet alle incidenten die kunnen plaatsvinden binnen een organisatie zijn echter informatiebeveiligingsincidenten. Maar, toch is dit heel vaak wel het geval. Informatiebeveiliging gaat over het waarborgen van de volgende drie aspecten:

- **Beschikbaarheid** beschrijft de beschikbaarheidsvereisten ten aanzien van de data die wordt gebruikt.
- **Integriteit** betreft de juistheid en volledigheid van de data die gebruikt wordt.
- **Vertrouwelijkheid** geeft aan wie toegang tot de data mag hebben en welke bevoegdheden hieraan gekoppeld zijn. (Bijvoorbeeld muteren, kopiëren, toevoegen, vernietigen of kennisnemen van informatie)

Hieruit blijkt dat informatie dus niet alleen beveiligd moet worden tegen actoren met een kwade intentie van binnen of buiten een organisatie. Ook incidenten zoals het niet opzettelijk wissen van gegevens, of een storing in het energienet of in een serverruimte gaan dus over informatiebeveiliging. Informatie is dan namelijk (tijdelijk) niet beschikbaar. Deze incidenten dienen dus ook als informatiebeveiligingsincidenten te worden behandeld.

1.2 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 incidentmanagementproces heeft dan ook als doel om ongeplande serviceonderbrekingen zo snel mogelijk te verhelpen.

Incidenten staan vaak niet op zichzelf en kunnen een uitwerking hebben naar andere belanghebbenden. 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 Ilionx. Indien nodig kunnen we ook escaleren richting het Nationaal Cyber Security Centrum (NCSC), zij hebben als Computer Emergency Response Team (CERT) het overzicht, de contacten en de middelen om andere overheden snel te kunnen waarschuwen.

2 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 bedrijfsvoering processen of schade ontstaan als gevolg van het incident te minimaliseren, dan wel te voorkomen.

2.1 Definities

Minor incident: Een minor incident heeft geen invloed op cruciale onderdelen van het systeem en zal ook niet eisen dat er extra controles moeten worden uitgevoerd. Minor incidenten vereisen geen interventie van hoger personeel of het management en er is geen melding van het event vereist.

Major incident: Een major incident treft kritische productiesysteem of -systemen, heeft verregaande gevolgen voor grote delen van de informatievoorziening 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. Major incidenten vereisen onmiddellijk handelen en de deelname van hoger personeel en het informeren van belanghebbenden zoals systeemeigenaren, leidinggevenden en het Response team.

Security incident: Een security incident is een verstoring die impact heeft op de dienstverlening, dit kan betrekking hebben op de beschikbaarheid van systemen of informatie) en/of het ongeoorloofd openbaren, verkrijgen en/of wijzigen van informatie (vertrouwelijkheid of integriteit van informatie of systemen). Een security incident kan zowel een Minor als Major incident zijn.

Privacy incident: Een security incident waarbij er toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens heeft plaatsgevonden, zonder dat dit de bedoeling was van de No. Een Privacy incident kan zowel een Minor als Major incident zijn.

2.2 Personeel

Het incidentmanagementproces 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 moeten gemeld worden aan de Chief Information Security Officer (CISO). Bij een escalatie of een noodsituatie moet altijd rekening gehouden worden met woordvoering waarbij Ilionx of eventueel het Nationaal Cyber Security Centrum (NCSC) advies kan geven. Al het personeel dat betrokken is bij het incidentproces 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. Onderstaand overzicht beschrijft de belangrijkste functionarissen bij een incident. Contactgegevens van de functionarissen en die van de betrokken leveranciers zijn beschreven in de checklist (zie bijlage 3). Deze checklist is offline en in hardcopy beschikbaar.

Stakeholder	Verantwoordelijkheid	Functionaris	Indien niet beschikbaar
Incident-manager	Beheren van het incidentmanagementproces en verantwoordelijk voor de communicatie binnen en eventueel buiten de No	Hoofd FD	Hoofd Bestuursbureau
Systeem-beheerder	Verzamelen van technische informatie en incident informatie	Systeembeheerder	Systeembeheerder
Helpdesk ICT	Verzamelen van technische informatie en incident informatie	Helpdesk ICT	Hoofd FD
CISO	Beoordelen en begeleiden van incidenten m.b.t inbreuk op de beschikbaarheid (>2uur) integriteit en vertrouwelijkheid.	CISO	FG
FG	Beoordelen en begeleiden van incidenten die tot een datalek kunnen of hebben geleid.	FG	CISO
Cyber Response leverancier	Verantwoordelijk voor het verzamelen en beschermen van bewijsmateriaal. Indien nodig ook voor het geven van advies m.b.t een incident.	Informatiebeveiliging advies (extern)	NCSC
MT-aanspreekpunt	Verantwoordelijk voor de communicatie naar het MT	Hoofd Bestuursbureau	Hoofd Communicatie en Omgevingsmanagement

	en bevoegd om beslissingen te nemen.		

2.3 Opzetten incidentmanagement

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

De volgende informatie is bedoeld als een algemene checklist van de stappen die de No 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 responseproces is de incidentmanager. De helpdesk heeft een nadrukkelijke rol bij het ontwikkelen van incidentresponsereacties en bij de voorbereiding daarop.

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

Een incident response-actie bestaat uit de volgende stappen:

1) identificatie;
2) schade indamming (insluiting en beperking);
3) remediatie en herstel;
4) kennisgeving, en;
5) rapportage en evaluatie.

2.3.1 Identificatie

Controleer of er een kwetsbaarheid aanwezig is en/of een incident daadwerkelijk heeft plaatsgevonden en registreer het incident.[1] 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 of via signalering door de monitoringsystemen iets naar boven komt.

2.3.2 Schade indamming

Nadat het incident is opgemerkt en gemeld gaat de ICT-helpdesk ermee aan de slag. De helpdeskmedewerker moet in het geval van een klein incident gaan handelen om de schade van het incident te beperken. Indien het incident groter is betrekt de helpdeskmedewerker de incidentmanager. De incidentmanager zal waar nodig een team aanstellen om het incident te

[1] Registratie van het incident vindt plaats in TopDesk.

verhelpen en zal hiervoor soms ook de CISO & FG nodig hebben. Bij grote informatiebeveiligingsincidenten zal de manager Bestuursbureau 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 Ilionx of eventueel het NCSC 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. Volg indien er gegevens zijn gelekt het datalekkenproces.

2.3.3 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. Als er diensten zijn uitbesteed is het noodzakelijk om goede afspraken te maken met de leverancier om incidenten goed op te pakken.

2.3.4 Kennisgeving

Bepaal welke gegevens mogelijk zijn blootgesteld door het incident en stel de getroffenen in kennis van het feit dat hun gegevens blootgesteld zijn. Informeer indien noodzakelijk andere overheidsinstanties, zoals het NCSC en/of de politie. Betrek voor deze melding eventueel een jurist. 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 aansprakelijkheid van de Nationale ombudsman.

2.3.5 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. Incidenten moeten goed worden opgeschreven, met de oplossing erbij, en bewaard zodat het incidentmanagementproces 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.

2.4 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),

remediatie van de oorzaak en het herstel van de functie (stap 3) kan worden gestart, terwijl documentatie activiteiten van stap 2.7 worden uitgevoerd (zie bijlage 1 voor een uitgebreide beschrijving van de stappen die gelden bij een major incident of een ernstig security incident).

Het is verstandig om de paraatheid van de Nationale ombudsman op het gebied van 'security 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.

Het stappenplan 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 Nationale ombudsman. 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. In de praktijk zijn de meeste incidenten 'minor incidenten'. Ook deze incidenten moeten geregistreerd en netjes afgehandeld worden. Een op het 'minor incident' proces toesneden stappenplan is opgenomen in bijlage 2.

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 gegevens, dient de Nationale Ombudsman rekening te houden met de gedeelde verantwoordelijkheid voor de incident response. Dit is 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 beveiliging gerelateerde termen van het contract tussen de Nationale ombudsman en die partij.

3 Aandachtspunten

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

3.1 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 responsedienst die detecteert of er kwetsbaarheden of incidenten hebben plaatsgevonden. Los van de detectie, worden logs ook veelvuldig achteraf gebruikt bij het reconstrueren van een incident of om te ontdekken welke systemen nog meer geraakt zijn. 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 logs op de juiste wijze bewaard en behandeld worden, kunnen logs ook dienen als bewijsmateriaal voor de wet. Let hierbij wel op dat logs persoonsgerelateerde of privacygevoelige informatie kunnen bevatten, en dat logs zodanig bewaard moeten worden dat deze niet zomaar kunnen 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.

3.2 Voorbereiding

Rond incidenten kunnen voorbereidingen getroffen en geoefend worden. Voor incidenten met een mogelijke hoge impact is het wenselijk om dat regelmatig te doen.

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).

3.3 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. 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.

3.3.1 Gouden tips

1) Vraag bij twijfel advies van een digitaal forensisch expert. Eventueel kan de 24-uurshulp van het NCSC worden gebeld.
2) Volg uw standaardprocedures.
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 gecompromitteerd 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.

4 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 incidentprioritering 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 incidentmaatregelen.

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.

4.1 Incident urgentie

In deze paragraaf worden urgentie categorieën verder uitgewerkt.

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.

4.2 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, het Ombudsplein moet gesloten worden.
	• Betrokkenen, bijvoorbeeld indieners van klachten en/ of verzoeken zijn geraakt en/of lijden schade, op welke wijze dan ook, als gevolg van het incident. Gevoelige Persoonsgegevens zijn gecompromitteerd.
	• De financiële impact van het incident is (naar schatting) 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 betrokkenen, bijvoorbeeld indieners van klachten en/ of verzoeken 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 (naar schatting) 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 betrokkenen, bijvoorbeeld indieners van klachten en/ of verzoeken zijn geraakt en/of lijden schade, maar dit is zeer minimaal. Persoonsgegevens zijn gecompromitteerd. • De financiële impact van het incident is (naar schatting) lager dan €1.000,- • Er is geen kans op reputatieschade.

4.3 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

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

4.3.1 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.

4.3.2 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).

4.3.3 Het identificeren van kritische incidenten

Hoewel helpdeskmedewerkers 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 Nationale ombudsman 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.

4.3.4 Belangrijkste eigenschappen van kritische incidenten

Enkele belangrijke gevolgen van kritische incidenten zijn:

- een groot aantal gebruikers/klanten kan 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 valt uit of is niet benaderbaar;
- de kosten (inclusief gevolgschade) voor gebruikers/klanten of voor de Nationale ombudsman 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 Nationale ombudsman zou reputatieschade kunnen oplopen; en:
- de tijd en moeite die nodig zijn om het incident op te lossen waarschijnlijk groot zijn en, indien afspraken zijn vastgelegd in SLA's, het zeer waarschijnlijk is dat afspraken die zijn vastgelegd in die SLA niet kunnen worden nagekomen.

Een kritisch incident kan ook worden omschreven als een ‘major (groot) incident’ of een ‘incident met hoge prioriteit’.

Bijlage 1: Major & Security incident stappenplan

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.**				
Soort incident[2]	*Gedaan*	***Taak***	***Eigenaar***	***Notities***
Ma, S,		1.1 Onmiddellijk blootstelling of schade beperken: - Voorbeeld: Als een elektronisch apparaat is gecompromitteerd: o Niet gebruiken (niet inloggen) of wijzigen van het apparaat o Zet het apparaat niet uit o Haal de netwerkverbindingen er af, maar NIET de voedingskabel (zet het apparaat op 'vliegtuigstand') 1.2 Registreer de melding als incident - 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.	Lijnmanager (Leidinggevende) voor het borgen dat dit proces wordt gevolgd en ICT voor de mogelijke afhandeling.	

[2] Toelichting op 'soort incident':
- Major incident: Ma
- Security incident: S

Ma, S		1.3 Waarschuw onmiddellijk de incidentmanager en de CISO *Handleiding: Voeg namen en telefoonnummers, e-mailadressen toe en zorg dat deze online en offline beschikbaar zijn. .*	Automatisch proces binnen Topdesk.	
Ma, S (indien van toepassing)		1.4 Indien er data of elektronische apparatuur gestolen of verloren is, dan ook aangifte laten doen door de gebruiker of eigenaar van het apparaat bij de politie. *Handleiding: Deze stap alleen uitvoeren na overleg en op advies van de CISO of ICT- afdeling.*	Gebruiker / eigenaar	
Ma, S		1.5 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:* *a) Hoofd Bestuursbureau* *b) Hoofd C&O (Persvoorlichting)* *c) NCSC* *d) Directeur (eindverantwoording)* *e) Ambtsdrager (via directeur/ MT-lid)* - Start met een logboek waarin gedurende het incident alle activiteiten op datum en tijd kunnen worden vastgelegd. - Indien het incident ook het lekken of verlies van persoonsgegevens betreft, leg dit dan nu vast en meld dit bij de Functionaris Gegevensbescherming.	CISO of incidentmanager	

Ma, S (indien van toepassing)		1.6 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.	Incidentmanager	
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.**				
Ma, S		2.1 Stel het Incidentresponseteam 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	

Ma, S		2.2 Beoordeling Incidentresponseproces en de verantwoordelijkheden met het Incidentresponseteam
		• Verstrek ieder teamlid het huidige incidentmanagement stappenplan.
		• Vindplaats stappenplan:
		  ○ Serverruimte en receptie (fysiek)
		  ○ DMS, offline op laptop (digitaal)
		• Bespreek de communicatiestrategie.
		  ○ Communicatie binnen de organisatie
		  ○ Woordvoerderslijn naar buiten
		• Bespreek het belang van het goed in een tijdlijn documenteren en het voorkomen van het verloren raken van onderzoeksgegevens.
			De manager van het Incident response team/ incidentmanager	

		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:* *a) Teamleden mogen niet praten met anderen buiten het team over het incident totdat er daarvoor toestemming is gegeven door het management of de CISO.* *b) Alle documentatie die door het team geschreven wordt moet op feiten gebaseerd zijn omdat het mogelijk in een strafrechtelijk onderzoek gebruikt kan worden.* *c) Er is dagelijks overleg tussen de teamleden.* *d) Het team moet bijhouden hoeveel tijd er besteed wordt en waaraan.*		
Ma, S		2.3 Verzamelen en veiligstellen van bewijsmateriaal *Handleiding: Verzamel fysiek en digitaal bewijs die tezamen een duidelijke, gedetailleerde beschrijving geven van hoe het incident heeft kunnen plaatsvinden (bijvoorbeeld: hoe de data gecompromitteerd kon worden).* *Voorbeelden:* *a) Images van de harddisk(en)* *b) Netwerkverkeersgegevens van en naar de gecompromitteerde apparatuur* *c) Werkplek applicatie logs* *d) Toegangslogs*	Incident response team	

		e) Foto's van de omgeving waar het incident plaatsvindt		
S		2.4 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:* *a) Beschrijf wat exact het bewijsmateriaal is.* *b) Leg vast wie erbij moest en waarom.* *c) Leg vast waar en hoe het bewijsmateriaal opgeslagen is.* *- Kluis; 2 sleutels gaan bij een incident naar de incidentmanager.* *d) 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	
Ma, S (indien van toepassing)		2.5 Neem maatregelen om de scope en de impact van het incident in te perken. *Voorbeelden:* *a) 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*	Incident response team	

		gecachte[3] *of in proxy opgeslagen webpagina('s), die geïndexeerd zijn door zoekmachine bedrijven en andere Internet-archief bedrijven, zoals bijvoorbeeld de Wayback Machine.* *b) Verander mogelijk gecompromitteerde wachtwoorden.* c) *Staak de exploitatie van een gecompromitteerde applicatie of server.*		
S		2.6 Voer forensisch onderzoek uit – of laat dit uitvoeren – 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 (indien extern: in overleg met inkoop)	
Ma, S		2.7 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	
Ma, S (indien van toepassing)		2.8 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	Functionaris Gegevens-bescherming	

3 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.

		een voormelding gedaan worden bij de Autoriteit Persoonsgegevens.		
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.**				
Ma, S		3.1 Ga terug naar stap 2.4 en zoek naar aanvullende manieren om de blootstelling te beperken. *Voorbeelden:* *a) Run periodiek web-queries om u er van te verzekeren dat de data niet verder is verspreid of gecached.* *b) Beoordeel de inventarisatie van getroffen hardware en systemen en wijzig verder waar nodig de wachtwoorden die mogelijk gecorrumpeerd zijn.* c) *Stop eventueel gecorrumpeerde diensten of applicaties en zorg voor work-arounds*	Incident response team	
Ma, S		3.2 Verwijder of mitigeer kwetsbaarheden van systemen, beoordeel toegangsrechten en remediatie risico's voor gevoelige dataopslag *Voorbeelden:* *a) Run vulnerability scans op getroffen systemen;* *b) Beoordeel en bepaal waar de data zich bevindt en wijzig dit indien nodig om een hogere beschermingsgraad te verzekeren.*	Incident response team	

		c) *Beperk de toegang tot systemen tot uitsluitend degenen die toegang nodig hebben.* d) *Gebruik software tools om gevoelige data te vinden, te verwijderen en te beschermen, bijvoorbeeld: Identity Finder.* e) *Herstel de getroffen objecten.*		
Ma, S		3.3 Als het onderzoek naar de bewijslast op de gecompromitteerde systemen klaar is kunnen ze weer in gebruik genomen worden.	Incident response team	
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 het NCSC 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.**				
Ma, S		4.1 Neem beslissingen op basis van de bevindingen van het Incident response team - Leidt het incident tot een beperkte beschikbaarheid van kritische informatiesystemen of tot een inbreuk op integriteit of vertrouwelijkheid van kritische gegevens? En geeft de mate van risico blootstelling de noodzaak tot het informeren van getroffenen?[4] - Zo ja, • Indien van toepassing, is het de taak van rechtshandhaving om de betrokken partijen te infomeren?	Incidentmanager	

4 Bijvoorbeeld bij niet versleutelde persoonsgegevens die gelekt zijn.

		• 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 Nationale ombudsman? - Als er geen kans is geweest op blootstelling van informatie aan buitenstaanders, dan kan eventueel meteen doorgegaan worden naar stap 4.5.		
Ma, S (Indien van toepassing)		4.2 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. Is er sprake van een hoog risico voor betrokkenen dan dienen deze ook in kennis gesteld te worden.[5] *Handleiding:* *Indien er persoonsgegeven betrokken zijn bij het incident zie dan het datalekken protocol.*	Management en Functionaris gegevensbescherming	
Ma, S		4.3 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.	Incidentmanager samen met CenO, geadviseerd door de CISO of door het Incident response team	

5 Art 33 en 34 van de AVG:Melding van inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit en mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene..

Ma, S (Indien van toepassing)		4.4 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:* *a) Websites worden vooral gemaakt als het aantal getroffenen te groot is of omdat niet alle mensen bekend zijn.* *b) De website content moet goedgekeurd worden.*	Incidentmanager samen met CenO, geadviseerd door de CISO of door het Incident response team	
Ma, S (Indien van toepassing)		4.5 Voorbereiding schriftelijke informatieverstrekking aan getroffenen: - Bedenk het onderwerp. - Schrijf een concept tekst in de huisstijl. *Handleiding:* *De inhoud van de brief moet zijn goedgekeurd door het management en door voorlichting.*	Incidentmanager geadviseerd door de intern klachtenbehandelaar, CenO en de CISO of door het Incident response team	
Ma, S (Indien van toepassing)		4.6 Als er een noodzaak of een verplichting is, informeer de politie en doe aangifte.	Management	
S		4.7 Informeer het NCSC.	CISO na afstemming met het management	

Ma, S (Indien van toepassing)		4.8 Doe de definitieve melding aan de Autoriteit Persoonsgegevens (AP) als er bij Stap 2.8 een voormelding 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.)	Functionaris Gegevensbescherming	
Ma, S (Indien van toepassing)		4.9 Informeer derde partijen zoals service providers als hiermee het risico van identiteitsdiefstal verkleind kan worden of als dat is vastgelegd in het respectievelijke contract.	Afhankelijk van het type leverancier: CenO of Inkoop	
Ma, S (Indien van toepassing)		4.10 Als er bankgegevens blootgesteld zijn aan niet rechthebbenden, informeer dan de bank of creditcard firma's.	Controller	
Ma, S		4.11 Coördineer de gelijktijdige communicatie-acties zodat de verschillende informatiestromen gelijktijdig plaatsvinden.	CenO (Voorlichting)	

Bijlage 2: Minor incident stappenplan

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 moet het incident geregistreerd worden en afgehandeld.**		
Taak	***Eigenaar***	***Notities***

1.7 Onmiddellijk blootstelling of schade beperken:
- Voorbeeld: 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 (zet het apparaat op 'vliegtuigstand')
 	
1.8 Registreer de melding als incident
- 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.
	Lijnmanager (Leidinggevende) voor het borgen dat dit proces wordt gevolgd en ICT voor de mogelijke afhandeling.	

STAP 2: Schade indamming en beoordeling van de blootstelling **In deze stap worden de noodzakelijke maatregelen getroffen om de schade van het incident te beperken en eventuele herhaling te voorkomen. Schat in of het nuttig of noodzakelijk is om betrokken medewerkers te informeren en handel hier naar.**		
2.2 Indien dit nuttig of noodzakelijk is: informeer betrokken medewerkers of de organisatie.	Incident response team	

2.8 Neem maatregelen om de scope en de impact van het incident in te perken. *Voorbeelden:* *d) 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 of in proxy opgeslagen webpagina('s), die geïndexeerd zijn door zoekmachine bedrijven en andere Internet-archief bedrijven, zoals bijvoorbeeld de Wayback Machine.* *e) Verander mogelijk gecompromitteerde wachtwoorden.* *f) Staak de exploitatie van een gecompromitteerde applicatie of server.*	Incident response team	
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.**		
3.4 Verwijder of mitigeer kwetsbaarheden van systemen, beoordeel toegangsrechten en remediatie risico's voor gevoelige dataopslag	Incident response team	
3.5 Als het onderzoek naar de bewijslast op de gecompromitteerde systemen klaar is kunnen ze weer in gebruik genomen worden.	Incident response team	
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 het NCSC 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.**		
4.12 (optioneel) Als er een noodzaak of een verplichting is, informeer de politie en doe aangifte.	Management	

Bijlage 3: Checklist Incident response

Stakeholder	Verantwoordelijkheid	Contactgegevens	Indien niet beschikbaar
Incidentmanager	Beheren van het incidentmanagementproces en verantwoordelijk voor de externe communicatie	Ger Slagboom +31 6 55 89 60 71 G.Slagboom@nationaleombudsman.nl	Dorien Sanders +31 6 11 51 36 57 D.Sanders@nationaleombudsman.nl
Systeembeheerder	Verzamelen van technische informatie en incident informatie	Jorryt Logtenberg +31 6 52 00 64 11 +31 70 356 35 62 j.logtenberg@nationaleombudsman.nl	Karin Schipperheijn +31 6 46 32 11 09 +31 70 356 36 78 k.schipperheijn@nationaleombudsman.nl
Helpdesk ICT	Verzamelen van technische informatie en incident informatie	Ricky Zwartbol +31 6 15 44 99 31 +31 70 356 36 90 r.zwartbol@nationaleombudsman.nl	ICT (dit gaat automatisch: Chris Geerlings, Jorryt Logtenberg en Karin Schipperheijn)
CISO	Beoordelen en begeleiden van incidenten m.b.t inbreuk op de beschikbaarheid (>2uur) integriteit en vertrouwelijk.	Matthijs Kerkvliet +31 6 50 15 47 13 m.kerkvliet@nationaleombudsman.nl	Andrik Eker +31 6 51 59 00 70 a.eker@nationaleombudsman.nl
FG	Beoordelen en begeleiden van incidenten die tot een datalek kunnen of hebben geleid.	Andrik Eker +31 6 51 59 00 70 a.eker@nationaleombudsman.nl	Matthijs Kerkvliet +31 6 50 15 47 13 m.kerkvliet@nationaleombudsman.nl
Cyber Response leverancier	Verantwoordelijk voor het verzamelen en beschermen van bewijsmateriaal. Indien nodig ook voor het geven van advies m.b.t een incident.	Ilionx 088 05 90 500	NCSC 070 751 55 55 info@ncsc.nl **bij nood: cert@ncsc.nl of 070 751 5021**
Webcare en Social Media	Verantwoordelijk voor communicatie over incidenten	Website No: Judith Laeven +31 70 356 35 10 J.Laeven@nationaleombudsman.nl	

	(bereikbaarheid No) naar buitenwereld	Website KOM: Nanou van der Elst +31 70 850 69 52 Nanou.vanderElst@dekinderombudsman.nl Socials: Lara Wittkowski +31 70 850 69 13 L.Wittkowski@nationaleombudsman.nl,	Socials: Lojs de Pooter +31 70 850 69 56 L.dePooter@nationaleombudsman.nl, en Marit Berghout +31 70 356 36 83 M.Berghout@nationaleombudsman.nl
MT-aanspreekpunt	Verantwoordelijk voor de communicatie naar het MT en bevoegd om beslissingen te nemen.	Dorien Sanders +31 6 11 51 36 57 D.Sanders@nationaleombudsman.nl	Alexandra Straus +31 6 52 82 42 01 a.straus@nationaleombudsman.nl
VISMA Circle	Zaaksysteem Verseon	Service Center +31 (0) 46 - 420 93 22 https://circlesoftware.topdesk.net/	n.v.t.
Caesar	Oracle	tel: +31 (0) 88 2404200 info@caesarexperts.nl	n.v.t.
Proact	IT Infra (1e leverancier)	Hans van Buuren (Projectmanager) 06 12 21 75 19 Hans.van.buuren@proact.nl	Gino van Miltenburg (Accountmanager) 06 55 70 27 27 Gino.van.miltenburg@proact.nl Bertus Doppenberg (Directeur Service Operations) 06 57 33 40 18 Bertus.Doppenberg@proact.nl
Brunel	IT Infra (2e leverancier)	Loed Arts (servicemanager) 06 20546691 l.arts@brunel.net	Bart Posthumus (Managing consultant) 06 51 303 956 b.posthumus@brunel.net
AskRoger	Telefonie	Support & servicedesk 088-2757610[6] support@askroger.nl	Peter Berg (Accountmanager) 088-2757646 of 06-12923294
SWIS	Website No & Website KOM	Rick van Haasteren (Teamleider) 071-5761323 rick@swis.nl	Menno de Kort (Senior Accountmanager) 06-51292055 menno@swis.nl

[6] De No heeft geen 24x7 supportcontract bij AskRoger