Procedure incidentenbeheer informatieveiligheid

Inhoudsopgave

1. Inleiding

Naast bewustwording en bedrijfscontinuïteit is het beheer van informatiebeveiliging het belangrijkste aandachtsgebied van informatiebeveiliging. De vraag is niet zozeer of er een beveiligingsincident met een hoge impact zal plaatsvinden, maar wanneer. Beveiligingsincidenten kunnen leiden tot tijdelijke discontinuïteit van de bedrijfsvoering, reputatieschade en grote financiële schade als gevolg van het bestrijden van een incident en het herstellen naar een normale situatie met mogelijke schadeclaims als sprake is van nalatigheid of van inbreuk op de beveiliging van persoonsgegevens.

Als het gaat om inbreuk op de beveiliging van, of verlies van persoonsgegevens is de meldplicht datalekken van toepassing als onderdeel van de Algemene Verordening Gegevensbescherming (AVG). De meldplicht vereist dat de organisatie een datalek direct meldt bij de Autoriteit Persoonsgegevens (AP) en aan betrokkenen wier persoonsgegevens het betreft. Dit laatste voor zover niet uitgesloten kan worden dat persoonsgegevens versleuteld of ontoegankelijk zijn voor degene die geen recht heeft op inzage in deze gegevens. Als de organisatie hierin verzuimt of tekortschiet dan loopt de organisatie een aanzienlijk boeterisico.

Dit vraagt om een structurele borging van het beheer van informatiebeveiligingsincidenten. Hierbij rekening houdend met de eisen die gesteld worden aan de meldplicht datalekken, die hiermee raakvlakken heeft. Dit document behandelt de organisatie en activiteiten die nodig zijn voor een goed werkend incidentenbeheer. De nadruk ligt op snel, doeltreffend en efficiënt reageren op het bestrijden en afhandelen van een beveiligingsincident.

Waar in dit stuk manager staat, kan zowel directeur als manager gelezen worden.

2. Doel, afbakening en doelgroep

Incidentenbeheer is het geheel van organisatorische maatregelen dat ervoor moet zorgen dat een incident op de juiste manier ontdekt, gemeld en behandeld wordt. Zo wordt de kans op uitval van de bedrijfsvoering of schade ontstaan als gevolg van het incident zo klein mogelijk gemaakt / gehouden of voorkomen. Een incident is een gebeurtenis, die de bedrijfsvoering negatief kan beïnvloeden.

Incidentenbeheer gaat ook over het opsporen van incidenten. Dat vereist dat de organisatie voldoende maatregelen heeft getroffen om zoveel mogelijk incidenten in beeld te kunnen krijgen. Dit kan door onder meer gebruik te maken van logging en controle daarop, antivirussoftware en een actief werkend Intrusion detection systeem (IDS) op het data netwerkverkeer. Daarnaast moet personeel getraind zijn op het herkennen van beveiligingsincidenten en moeten zij weten wat zij moeten doen.

De procedure incidentenbeheer heeft betrekking op alle medewerkers en uitzendkrachten, die werkzaam zijn bij de organisatie en op ketenpartners en bewerkers (persoonsgegevens) waar uitwisseling van informatie plaatsvindt. Dit alleen als de verantwoordelijkheid voor het oplossen van een incident en herstel naar een normale situatie bij de organisatie ligt.

Buiten het aandachtsgebied:

Gelet op de verscheidenheid van mogelijk te ontdekken incidenten blijft opsporing van beveiligingsincidenten buiten de scope van dit document. De procedure incidentenbeheer begint bij de melding van een incident.

Als blijkt dat een incident uit de hand dreigt te lopen en daardoor de bedrijfscontinuïteit ernstig in gevaar kan komen, dan vindt direct opschaling plaats naar het zorgcontinuïteitsplan. Het opschalen naar een dergelijk plan valt buiten de scope van dit document.

3. Verantwoordelijkheden, controle en referenties

Namens de directie die eindverantwoordelijk is binnen de organisatie, is de FG eigenaar van dit document en verantwoordelijk voor het actueel houden van dit document, voor archivering en distributie naar de organisatie en voor implementatie en naleving.

Dit document treedt in werking na formele vaststelling door het managementteam van de organisatie.

Indien naleving van dit document getest wordt, behoort aandacht te worden besteed aan:

- Beoordelen registratie van incidenten
- Afhandeling van incidenten en in het bijzonder datalekken
- Dossiervorming
- Rapportage aan management

4. Organisatie incidentenbeheer

4.1. Inleiding

Incidentenbeheer is structureel ingebed in de interne organisatie van de organisatie Eilandzorg. Naast het melden en afhandelen van beveiligingsincidenten is periodieke rapportage over incidentenbeheer aan het management belangrijk vanwege nadelige gevolgen van incidenten. Zo'n overzicht geeft een indicatie over de mate van informatiebeveiliging bij de organisatie, hoewel niet alle beveiligingsincidenten veroorzaakt worden door nalatigheid of tekortkomingen in de beveiliging. Het helpt de organisatie in ieder geval het beveiligingsniveau waar nodig aan te passen. Het biedt concrete voorbeelden voor het verhogen van de bewustwording bij personeel over informatiebeveiliging.
De FG is verantwoordelijk voor het periodiek verstrekken van informatie over beveiligingsincidenten.

4.2. ICT

De FG registreert de binnenkomende incidenten en handelt deze in de meeste gevallen ook af. Het gaat dan in veel gevallen om incidenten waarvan de melder zelf last heeft en waarvan de impact gering is. Bij afhandeling kan, afhankelijk van de aard van het incident, hulp ingeroepen worden van een mt lid of externe ict.

4.3. Crisis Beleids Team (CBT)

Eilandzorg heeft een CBT ingesteld om voorbereid te zijn om snel en adequaat te kunnen reageren op een beveiligingsincident die buiten de scope van de ICT valt. Het gaat dan om beveiligingsincidenten met een hoog of kritische classificatie die directe mobilisering van het CBT vereist. Criteria voor het mobiliseren van het CBT zijn beschreven in hoofdstuk 7.
Het managementteam heeft de vaste kern van het CBT benoemd. Verder wordt verwezen naar het Zorgcontinuïteitsplan.
Afhankelijk van de aard, omvang en impact van het incident kunnen de volgende teamleden dan wel disciplines worden toegevoegd:

- vertrouwensfunctionaris ingeval sprake is van verwijtbaar gedrag van een medewerker die een incident heeft veroorzaakt;

- juridische bijstand om de gevolgen van een incident juridisch te toetsen. Denk aan aansprakelijkheid en boetes (Wbp/AVG);
- externe inhuur indien bijzondere expertise nodig is zoals een ICT-specialist of een digitaal forensisch expert;
- financieel specialist om de schadekosten in beeld te brengen en na te gaan in hoeverre de schade verzekeringstechnisch is afgedekt en de financiële claim afwikkelt;
- afdeling communicatie om mogelijke reputatieschade zoveel mogelijk in te dammen en direct te werken aan reputatieherstel.

Deelname van inhuurkrachten aan het CBT vereist dat zij vooraf een integriteits- en geheimhoudingsverklaring hebben ondertekend.

5. Procedure

5.1. Inleiding

Een succesvolle afhandeling van incidenten bestaat uit een aantal te doorlopen processtappen die voor elk incident gelijk is. De verschillen zitten voornamelijk in de details (inhoud). Van belang is dat de organisatie beschikt over een draaiboek waarin diverse beveiligingsincident zijn opgenomen om bepaalde type incidenten snel en efficiënt te kunnen afhandelen.

Elke medewerker moet alert zijn op bedreigingen met betrekking tot informatiebeveiliging en is verplicht om elk beveiligingsincident die hij/zij ontdekt of vermoedt te melden. Dit is ook opgenomen in het arbeidscontract. Daarbij geldt uiteraard dat elke medewerker in staat moet zijn een beveiligingsincident te kunnen herkennen en weet hoe en waar hij moet melden. De drempel voor het melden van een incident moet laag te zijn. De FG zorgt ervoor dat informatie over het herkennen van beveiligingsincidenten (voorbeelden) en hoe gemeld behoort te worden beschikbaar is via daarvoor bestemde communicatiekanalen van de organisatie.

Voorbeelden van beveiligingsincidenten zijn:

- Verlies of diefstal van waardepapier, dossier, usb-stick, tablet of andere gegevensdragers
- Niet naleven van beleid of richtlijnen
- Inbreuk op fysieke beveiligingsvoorzieningen
- Toegangsovertredingen / ongeoorloofd gebruik van sleutels
- Opzettelijk foutief handelen (fraude, diefstal)
- Beschadigen of vernielen van (kritische) apparatuur
- Virusbesmetting als gevolg van het aanklikken van een onbetrouwbare bijlage
- Onbevoegd inzien van vertrouwelijke informatie
- Onbedoelde openbaarmaking van vertrouwelijke informatie
- Geen gescreend personeel
- Illegale licenties
- Illegaal kopiëren van gegevens
- Email met niet versleutelde vertrouwelijke informatie / het niet gebruiken van zorgmail
- Kenbaar maken van of onzorgvuldig omgaan met wachtwoorden
- Praten in openbare ruimtes over cliënten- / personeelsgegevens
- Een groepsapp, waarbinnen cliënten worden besproken
- Medicijnlijsten, clientgegevens, zorgplannen die op de printer blijven liggen

Maar ook cyberaanvallen zoals een ddos, computerhacking of besmetting met ransomware, of het

technische falen van apparatuur, stroomuitval, wateroverlast en dergelijke zijn aan te merken als incidenten.

5.2. Meld intern en prioriteer

De FG is het aangewezen meldpunt en registreert alle incidentmeldingen. Een centraal meldingspunt is van belang om het proces zoveel mogelijk te standaardiseren, om versnippering van geregistreerde meldingen te voorkomen en om het totaaloverzicht te behouden(volledigheid). Alle meldingen worden daar geregistreerd.
Het registratiesysteem is beveiligd tegen ongeautoriseerde toegang.
Alle incidentmeldingen zijn voorzien van een urgentie- en impactcode en gecategoriseerd voor rapportage doeleinden. Hiervoor zijn nadere instructies aanwezig die de FG onderhoudt. De basis voor prioritering ligt vast in hoofdstuk 7.
De ICT is geïnstrueerd voor het direct doorgeven van incidenten aan de directie die buiten hun scope vallen.

5.3. Mobiliseer CBT

De vaste kern van het CBT wordt gemobiliseerd als een incident is afgegeven met een hoge of kritische impact. Men beoordeelt direct de aard en omvang van het incident en stelt vast of het incident ook daadwerkelijk heeft plaatsgevonden, bijvoorbeeld door contact op te nemen met systeembeheer of de melder van het incident. Ze moeten snel inzicht krijgen in:

- de aard en omvang van het incident,
- welke teamleden aanvullend opgenomen moeten worden in het CBT en
- welke instanties geïnformeerd moeten worden over het incident (tenminste AP).

Het CBT is belast met het beperken van verdere schade als gevolg van het incident, het blokkeren of verwijderen van de oorzaak, stelt de schade vast en zorgt voor het veiligstellen van bewijsmateriaal. Van elk incident dat via het CBT loopt vindt dossiervorming plaats. Het CBT maakt hierbij zoveel mogelijk gebruik van kennis en ervaring en voorbereidingen die zijn vastgelegd in een daarvoor opgesteld draaiboek (zie ook 4.3).

Het CBT bepaalt welke acties noodzakelijk zijn. Voor elk te behandelen incident via het CBT geldt dat teamleden niet mogen praten met anderen buiten het team totdat daarvoor toestemming is gegeven door de FG. Dit om zoveel mogelijk ruis in de communicatie te voorkomen.

De FG onderhoudt het contact met de directie over de stand van zaken betreffende het incident. De directie informeert indien nodig het bestuur.

5.4. Beperk schade en elimineer oorzaak

Er wordt zo snel mogelijk gestart met het indammen van de schade door het incident te blokkeren, te verwijderen en de impact voor verdere blootstelling te verminderen. Dit kunnen zowel activiteiten zijn vanuit de techniek als vanuit de organisatie. Vanuit de techniek is de TD belast met het indammen van de schade en blokkeren of verwijderen van de oorzaak eventueel ondersteunt met externe expertise. Daarbij maakt het team waar nodig gebruik van vooraf opgestelde escalatieprocedures uit het zorgcontinuïteitsplan. Deze onderdrukkende handelingen kunnen leiden tot tijdelijke uitval van onderdelen van het ICT-netwerk en/of verlies van data om verdere schade te voorkomen.

Het CBT bepaalt in samenspraak met de manager en afdeling communicatie de (interne en externe) communicatiestrategie. Intern kan dit gericht zijn op het melden van het incident met bijbehorende instructies om bepaalde handelingen tijdelijk niet uit te voeren met eventueel een voorlopig spreekverbod om escalatie zoveel mogelijk te voorkomen. Extern is de communicatie gericht om zoveel mogelijk reputatieschade te voorkomen en direct te werken aan reputatieherstel. Externe communicatie gebeurt altijd in overleg met de directie.

Voor het veiligstellen en verzamelen van bewijslast kan eventueel externe expertise nodig zijn. Indien sprake is van (mogelijke) inbreuk op de beveiliging van persoonsgegevens behoort het datalek direct te worden gemeld bij de AP en eventueel aan betrokkenen. Dit traject loopt altijd via de FG. Zie hiervoor verder hoofdstuk 6.
Het CBT bepaalt aan de hand van de aard van het incident en in overleg met een jurist of aangifte bij de politie gedaan moet worden (strafrechtelijk onderzoek).

5.5. Herstel oude situatie

Na het indammen van de schade en het verwijderen van het incident is zo spoedig mogelijk herstel naar de oude situatie nodig. Bij bedrijfsprocessen die (deels) gestopt zijn als gevolg van een incident vindt op een gecontroleerde wijze een herstart plaats. Eventueel verlies van data wordt gereconstrueerd bijvoorbeeld aan de hand van een recovery procedure en/of brondocumenten (opnieuw invoeren). Het herstarten van een bedrijfsproces geschiedt in nauw overleg met de manager.

In overleg met de manager vindt communicatie naar de organisatie plaats over het herstel en eventuele gevolgen ervan. De basis hiervoor is al gelegd in paragraaf 5.4.
De afdeling financiën brengt de directe en indirecte kosten als gevolg van de schade zoveel mogelijk in beeld, rekening houdend met mogelijk ingediende schadeclaims van derden. Verder wordt nagegaan in hoeverre deze kosten verhaald kunnen worden via de verzekering of derden of voor eigen rekening zijn. De afdeling financiën is eventueel in overleg met een jurist belast met de verdere financiële afwikkeling van het incident.

Als een medewerker van de organisatie betrokken is bij de oorzaak van een beveiligingsincident door nalatig of kwaadwillend gedrag en daarvoor het nodige bewijsmateriaal is veiliggesteld, wordt de vertrouwenspersoon ingeschakeld en eventueel aangifte gedaan bij de politie. De gevolgen hiervan voor de betrokken medewerker kunnen leiden tot disciplinaire maatregelen, strafrechtelijk onderzoek en/of tot ontslag. Voor betrokkenheid van een externe medewerker geldt eenzelfde procedure zonder dat er geen vertrouwensfunctionaris betrokken is, maar het contract ontbonden kan worden.

5.6. Informeer doelgroepen/betrokkenen

De afdeling communicatie probeert reputatieschade zoveel mogelijk in te dammen en richt haar communicatie op reputatieherstel.
Intern gaat het dan om de organisatieraad, bestuur, management en medewerkers en extern om ketenpartners, media en andere belanghebbenden. Hierbij wordt zoveel mogelijk gebruik gemaakt van standaard teksten in eigen huisstijl om geen tijd te verliezen waar snelheid geboden is.
Ingeval sprake is van een datalek wordt verwezen naar de meldplicht zoals opgenomen in paragraaf 6.3, 6.4 en 6.5.

5.7. Evalueer, rapporteer en documenteer

Het CBT verzamelt van elk beveiligingsincident waarop dossiervorming van toepassing is alle benodigde documentatie die nodig is voor bewijsvoering als sprake is van civiel of strafrechtelijk onderzoek, schadeclaims of toezicht vanuit de AP. Documentatie kan bestaan uit bespreekverslagen, ingevulde checklist, printscreens, emails, controle op loggings, bevindingen van ICT-specialisten of digitaal forensische experts, processen verbaal en de (uitwerking van de) communicatiestrategie.
Het CBT voert een evaluatie uit en legt dit vast in een rapportage inclusief advies ter verbetering. Het rapport wordt voorgelegd aan de directie en besproken. Waar nodig past de FG het incident draaiboek aan. De afdeling HRM bepaalt in hoeverre het beveiligingsincident kan worden opgenomen in het bewustwordingsprogramma van de organisatie.
Na afsluiting van het incident archiveert de FG het incidentendossier. Vernietiging van het dossier vindt plaats nadat de daarvoor geldende wettelijke bewaartermijnen zijn verlopen. Het dossier is vertrouwelijk tenzij de FG anders bepaalt.

6. Meldplicht datalekken

6.1. Inleiding

De AVG bepaalt dat datalekken direct, binnen 72 uur, gemeld moeten worden aan de Autoriteit Persoonsgegevens (’AP’), tenzij het onwaarschijnlijk is dat het datalek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen.
Daarnaast moet het datalek ook aan de betrokkenen gemeld worden als het waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen met zich meebrengt.

Aan de beantwoording van de vraag moet een zorgvuldige (belangen)afweging voorafgaan. Hierbij is bijvoorbeeld de aard en de omvang van de persoonsgegevens die gelekt zijn van belang. Als er bijzondere persoonsgegevens, zoals gegevens over gezondheid, gelekt zijn, dan is de melding meestal noodzakelijk.

Dit protocol datalekken is bedoeld als hulpmiddel voor de beantwoording van de vraag of er sprake is van een datalek en of deze gemeld moet worden.

6.2. Wat is een datalek?

Er is sprake van een datalek als er een inbreuk in verband met persoonsgegevens heeft plaatsgevonden. Alleen een dreiging of een tekortkoming in de beveiliging is niet voldoende; er moeten daadwerkelijk persoonsgegevens gelekt zijn.

Onder een datalek verstaat de AP persoonsgegevens die gelekt of vernietigd zijn als gevolg van een beveiligingsincident. Bij het lek zijn persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking.
Bij verlies zijn de persoonsgegevens er niet meer.
Onder onrechtmatige verwerking vallen bijvoorbeeld onbevoegde kennisneming, wijziging, aantasting of de verstrekking daarvan.

6.2.1. Contactpersoon aanwijzen

De organisatie heeft een contactpersoon aangewezen aan wie eventuele datalekken gemeld moeten worden (FG = functionaris gegevensbescherming).

6.3. Informeren medewerkers

Medewerkers binnen de organisatie moeten er van bewust te zijn dat als er sprake is van een datalek, zij dit datalek direct (diezelfde dag nog) moeten melden bij de FG, zodat deze het datalek op tijd kan melden bij de Autoriteit Persoonsgegevens. Medewerkers moeten bekend zijn met het in dit protocol opgenomen stappenplan.

6.4. Uitvoeren van het stappenplan Datalekken

De FG zorgt voor de invoering en naleving van het hieronder beschreven stappenplan Datalekken. Als er een datalek optreedt, dienen de stappen in het stappenplan Datalekken doorlopen te worden.

STAPPENPLAN DATALEKKEN

Processtappen	Activiteit	Verantwoordelijke persoon
1. Er wordt een (mogelijk) datalek ontdekt	- Maak direct melding van (mogelijke) datalek via privacy@eilandzorg.com - Informeer FG, die manager informeert	Medewerker die het ontdekt
2. Beoordeel het datalek	- Onderzoek het beveiligingsincident - Onderzoek of er persoonsgegevens verloren zijn gegaan of onrechtmatig gebruikt kunnen worden - Beoordeel wie of welke afdelingen binnen de organisatie hierbij betrokken zijn - Beoordeel of er een verwerker betrokken is bij het incident. Zo ja dan dient deze bij het proces betrokken te worden	Manager FG FG FG
3. Bestrijdt het datalek	- Stop het datalek als het nog kan - Neem andere maatregelen om het datalek en de daaruit voortvloeiende schade te beperkten - Leg de acties van de genomen maatregelen vast in het dossier	Manager Manager FG
4.Vaststellen impact datalek	- Onderzoek het datalek en de gevolgen daarvan - Onderzoek de aard van de gegevens die gelekt zijn. Bijv. gezondheidsgegevens, wachtwoorden, gegevens over financiële situatie of die kunnen leiden tot	Manager Manager

	vooroordelen/misbruik - Onderzoek de omvang van de gelekte gegevens - - Beoordeel welke impact het lek kan hebben op de betrokken personen - Stel vast wat de nadelige gevolgen kunnen zijn	 FG FG FG
5. Vaststellen Meld en Herstelaanpak	- Bepaal aanpak/informeren AP - Bepaal aanpak/informeren betrokkenen - Bepaal acties voor nazorg betrokkenen - Bepaal acties voor belang van de organisatie - Bepaal acties voor verbetering beveiliging	Manager Manager Manager Manager FG
6. Melden AP*	- Indien besloten wordt om AP te informeren dan moet dat binnen 72 uur - Melding via het meldloket: digitale formulier van de website van het AP - Tel nr AP: 0900-3282535	FG Manager FG
7. Melden betrokkenen**	- Melding via bijvoorbeeld brief - Meedelen wat er is gebeurd, welke persoonsgegevens getroffen zijn en wat de mogelijke gevolgen van het datalek kunnen zijn - Informeren over de maatregelen die de organisatie neemt en die de betrokkene zelf kan nemen om schade te voorkomen	FG Manager Marketing/communicatie
8. Uitvoeren herstelwerkzaamheden	- Herstel het datalek - Verbeteren van de beveiliging	ICT partner FG Marketing / communicatie

	- Lever nazorg aan de betrokkenen	
9. Optimaliseer het beveiligings- en het Datalek proces	- Registreer, evalueer en verbeter de beveiliging en het proces inzake melding datalekken	FG Manager

* Melding aan de Autoriteit persoonsgegevens kan alleen achterwege blijven, als het onwaarschijnlijk is dat het datalek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen. Of hiervan sprake is, hangt mede af van de aard en omvang van de gelekte persoonsgegevens. Als bijvoorbeeld uitsluitend de adresgegevens zijn gelekt van een kleine groep betrokkenen, dan is het onwaarschijnlijk dat er sprake is van een hoog risico. Dat is wellicht anders als de adresgegevens in combinatie met het lidmaatschap van de patiënten of cliëntenorganisatie zijn gelekt. Het lidmaatschap van de organisatie kan gezien worden als een gevoelig gegeven en de leden van de organisatie kunnen wellicht behoren tot een kwetsbare groep, die extra bescherming nodig heeft. Bij de afweging van het risico voor de rechten en vrijheden van de betrokken zal de Functionaris Gegevensbescherming altijd betrokken moeten worden.

** Als het datalek waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen veroorzaakt, moet het datalek ook aan de betrokkenen gemeld worden. Het risico zal bijvoorbeeld moeten worden beoordeeld aan de hand van de aard en de hoeveelheid van de gelekte gegevens. Als er persoonsgegevens van gevoelige aard (bijv. gezondheidsgegevens) gelekt zijn, zal het lek in ieder geval gemeld moeten worden aan de betrokkenen. Bij de afweging van het risico voor de rechten en vrijheden van de betrokkenen zal altijd de Functionaris Gegevensbescherming betrokken moeten worden.

6.5. Verwerkers

Het kan gebeuren dat het datalek optreedt bij de verwerker. De organisatie is en blijft (als verwerkingsverantwoordelijke) altijd verantwoordelijk voor het datalek bij de verwerker. In dat geval moet dus hetzelfde stappenplan worden afgewerkt. De verwerker zal bij de stappen betrokken moeten worden.

Via de verwerkersovereenkomst moet afgedwongen worden dat de verwerker eventuele datalekken direct (binnen 24 uur) meldt bij de organisatie en de organisatie helpt bij het beoordelen of er gemeld moet worden en de afwikkeling van het datalek. Belangrijk is dat de verwerker niet buiten de organisatie om een datalek meldt bij de Autoriteit Persoonsgegevens. De verwerker moet verder alle redelijke instructies van de organisatie opvolgen.

7. Prioritering incident

Om de geschikte incidentmaatregelen te activeren, gebruikt de organisatie een leidraad voor incidenten prioritering. Het gaat hierbij om twee factoren: urgentie en impact.
De urgentie is de maat voor hoe snel de oplossing van een incident vereist is en de impact is de maat voor de omvang van het incident en van de mogelijke schade als gevolg van het incident voordat het kan worden opgelost.

De organisatie hanteert de volgende criteria:

Urgentie	***Omschrijving***
Hoog	- De schade, veroorzaakt door het incident neemt snel toe. - Werk dat moet worden hersteld door medewerkers is zeer arbeidsintensief. - Een groot incident kan worden voorkomen door bij een klein incident onmiddellijk te handelen.
Medium	- De schade, veroorzaakt door het incident neemt in de tijd aanzienlijk toe. - Er gaat werk verloren, maar dit is relatief snel te herstellen.
Laag	- De schade, veroorzaakt door het incident neemt in de tijd maar weinig toe. - Het werk dat blijft liggen is niet tijdsintensief.

Impact	***Omschrijving***
Hoog	- 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 organisatie zijn geraakt en/of lijden schade, op welke wijze dan ook, als gevolg van het incident. Persoonsgegevens zijn hierdoor geschaad. - De financiële impact van het incident is hoger dan <€50.000,->. - Er is reputatie schade, de krant wordt gehaald.
Medium	- Sommige personeel is geraakt door het incident en/of kan zijn/haar werk niet meer doen, bijvoorbeeld een afdeling. - Enkele inwoners van een organisatie zijn geraakt en/of lijden schade, op welke wijze dan ook, als gevolg van het incident. Persoonsgegevens zijn hierdoor geschaad. - De financiële impact van het incident is hoger dan <€10.000,-> en lager dan <€50.000,->. - Er is kans op reputatie schade.
Laag	- Enkele personeelsleden zijn geraakt door het incident en/of kunnen niet meer hun werk doen. - Enkele inwoners van een organisatie zijn geraakt en/of lijden schade, maar dit is zeer minimaal. Persoonsgegevens zijn gecompromitteerd. - De financiële impact van het incident is lager dan <€10.000,-> - Er is geen kans op reputatie schade.

De Incident Prioriteit wordt verkregen door urgentie en impact tegen elkaar af te zetten. De incident prioriteit matrix ziet er als volgt uit:

	Impact			
		Hoog	*Midden*	*Laag*
Urgentie	*Hoog*	1	2	3
	Midden	2	3	4

	Laag	3	4	5

De kleurcodetabel[1] leidt tot de volgende classificatie:

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

Het CBT wordt gemobiliseerd indien de classificatie kritiek of hoog is.

8. Formele vaststelling

Het managementteam heeft dit document als eindverantwoordelijke formeel vastgesteld in de vergadering van 14 Juni 2018.

Aldus getekend,

Het MT