

**Bijlage 1 – Incidentenopvangplan**

**Versieblad**

Datum	Versie	Gemaakt door	Omschrijving van de aanpassing
DD/MM/JJJJ	0.1	Dejan Kosutic	Concept Basisdocument overzicht

**Comment [DK1]:** Om te leren hoe dit document in te vullen, zie deze **videohandleiding tutorial** "Video Tutorial: How to Write a Business Continuity Plan According to ISO 22301":  
 - Indien u de toolkit heeft gekocht, dan vindt u het in het ISO 27001 & ISO 22301 Klantenportaal: <https://epps.customerhub.net/>  
 - Indien u de toolkit niet heeft gekocht, dan vindt u de preview van de handleiding hier: <http://www.iso27001standard.com/business-continuity-plan-how-to-write-it-according-to-iso-22301>

**INHOUDSOPGAVE**

**1. DOEL, TOEPASSINGSGBIED EN GEBRUIKERS .....2**

**2. AUTORISATIES EN VERANTWOORDELIJKHEDEN IN INCIDENTENOPVANG .....2**

**3. COMMUNICATIE .....2**

**4. PROCEDURES VOOR VERSTORENDE INCIDENTEN .....3**

4.1. EEN VERSTOREND INCIDENT BEHEERSEN ..... 3

4.1.1. *Verplichting van elke werknemer om incidenten te melden* ..... 3

4.1.2. *Omgaan met een verstorend incident* ..... 3

4.1.3. *Crisismanager* ..... 4

4.2. BEHEERSEN EN TOTAAL OPlossen VAN EEN INCIDENT ..... 4

4.2.1. *Ontruiming van het gebouw (ongeacht het soort incident)* ..... 4

4.2.2. *Brand* ..... 5

4.2.3. *Onderbreking van stroomtoevoer* ..... 5

4.2.4. *Aardbeving* ..... 5

4.2.5. *Dreigbrief* ..... 6

4.2.6. *Dreigtelefoontje / bommelding* ..... 6

4.2.7. *Uitval telecommunicatie* ..... 7

4.2.8. *Uitval informatiesysteem* ..... 7

4.2.9. *Virusaanval* ..... 8

4.2.10. *Overtreding van de interne of externe regels* ..... 8

**5. REGISTRATIEBEHEER OP BASIS VAN DIT DOCUMENT .....8**

**6. GELDIGHEID EN DOCUMENTBEHEER .....9**

### 1. Doel, toepassingsgebied en gebruikers

Het doel van dit Plan is om de bescherming van de gezondheid of veiligheid van mensen in geval van een ramp of ander incident te waarborgen, of het incident te beheersen. De doelstelling is om de schade te verminderen naar de meest mogelijke omvang.

Dit Plan is van toepassing op alle grote incidenten die enige activiteit binnen het ISMS [BCMS] toepassingsgebied dragen te voorkomen langer dan de recovery point objective voor elke afzonderlijke activiteit (verderop in de tekst: verstorende incidenten).

Gebruikers van dit document zijn alle werknemers van [naam organisatie].

### 2. Autorisaties en verantwoordelijkheden in incidentenopvang

Rol in herstel / functie	Autorisaties en verantwoordelijkheden
Elke werknemer	De verantwoordelijke organisatie-eenheid waarschuwen over het incident
[functie] of werknemer in [naam van organisatie-eenheid]	Alle stappen noodzakelijk om de aanpak van communicatiegerelateerde incidenten op te lossen
[[functie] of werknemer in [naam van organisatie-eenheid]	Alle stappen noodzakelijk om alle andere incidenten op te lossen
[functie]	Beheer van de communicatie met de media
[functie]	Communicatie met de publieke media – deze persoon heeft als enige de verantwoordelijkheid te communiceren met de publieke media
[functie]	Psychische hulp voor werknemers

**Comment [DK2]:** Dient de in het Bedrijfscontinuïteitsplan genoemde persoon te zijn.

**Comment [DK3]:** Dient de in het Bedrijfscontinuïteitsplan genoemde persoon te zijn.

### 3. Communicatie

De volgende tabel vermeldt de verantwoordelijkheden voor communicatie (zowel sturen als ook het ontvangen van informatie en reageren op informatieaanvragen) met verschillende externe belanghebbenden:

	[Telefoon]	[E-mail]	[E-mail]	[Media]		
[Werknemers]						
[Familieleden werknemers]						
[Klant]						
[Relaties]						
[Hulpdiensten]						

**Comment [DK4]:** Dit gedeelte zou moeten worden uitgebreid met procedures aangaande een nationaal of regionaal dreigingadviesstelsel, indien zo iets dergelijks is geïdentificeerd in de Bedrijfscontinuïteit Strategie.

**Comment [DK5]:** Neem de verantwoordelijkheid te communiceren met de media gestart (onmiddellijk na een incident is opgetreden / nadat het te beheersen is geworden / nadat het is opgelost, enz.)

De communicatieprocedure gaat als volgt:

1. Een werknemer die een communicatieverzoek ontvangt of die communicatie wil opstarten richting een gereserveerde partij, dient een dergelijk verzoek door te geven aan de verantwoordelijke zoals aangegeven in de vorige tabel.
2. Een verantwoordelijke moet het eens zijn met [functie] over de inhoud van de communicatie
3. Indien de communicatie met externe partijen verband houdt, dient de verantwoordelijke goed tekeuren of de informatie te worden vrijgegeven en te worden goedgekeurd door [functie] voor dat dergelijke informatie wordt vrijgegeven
4. Na de verkregen toestemming, levert de verantwoordelijke de informatie aan de gereserveerde partij.

**Comment [DK6]:** Dient de in het Bedrijfscontinuïteitsplan genoemde persoon te zijn.

De verantwoordelijke genoemd in de vorige tabel is verantwoordelijk voor het vastleggen van elke communicatie met een gereserveerde partij.

#### 4. Procedures voor verstorende incidenten

**Comment [DK7]:** Neem hier alle incidenten op die als meest waarschijnlijk zijn beoordeeld in de risicobeoordeling.

##### 4.1. Een verstorend incident beheersen

###### 4.1.1. Verplichting van elke werknemer om incidenten te melden

Elke werknemer is verplicht om elk verstorend incident op de volgende manier te melden:

- alle aan IT- en communicatietechnologie gerelateerde incidenten worden telefonisch gemeld aan [functie] of naar een van de gereserveerde partijen
- alle andere incidenten worden telefonisch gemeld aan [functie] of naar een van de gereserveerde partijen

**Comment [DK8]:** Indien het karakter van het incident vereist, kan het ook worden gemeld via e-mail of door middel van een softwaretool.

Enig andere gebeurtenis of systeemkwetsbaarheid dat zich nog niet tot een verstorend incident heeft ontwikkeld, dient op dezelfde manier te worden gemeld.

**Comment [DK9]:** Indien deze kwestie al is geregeld door de Procedure voor Incidentbeheer volgens de ISO 27001, dan verwijder deze tekst en voeg een verwijzing toe naar de Procedure.

Indien een incident de tussenkomst van de politie, ambulance of brandweer vereist, dan dient de verantwoordelijke de gereserveerde partijen hiervan in kennis te stellen en de noodzakelijke maatregelen te nemen.

In geval date en incident optreedt, dan kunnen werknemers alleen vrijuit spreken met hun superieuren en de politie, ambulance, brandweer, tenzij alle andere communicatie met de crisismanager wordt overgelaten.

###### 4.1.2. Omgaan met een verstorend incident

De persoon die de informatie over een verstorend incident heeft ontvangen dient te beoordelen of het incident gereserveerd incident is of niet is, en indien wordt bepaald dat het is, dan dient het plan onmiddellijk te worden geactiveerd door de volgende stappen te nemen:

- begin met het beheersen en stoppen van het incident als beschreven in de komende gedeeltes van dit document
- breng alle verantwoordelijken op de hoogte van het optreden van het incident binnen hun verantwoordelijkheden
- breng [functie] op de hoogte, die moet overwegen of enig belangenpartij dient te worden gewaarschuwd
- bepaal de status van een incident en wanneer nodig, informeer de vertegenwoordigers van incidenten en andere betrokken werknemers over de voortgang in het omgaan met het incident

In geval dat een persoon niet in staat is het incident te beheersen of voorgoed op te lossen, dan dient hij/zij de crisismanager te informeren. De informatie die is doorgegeven naar de crisismanager dient de aard en de ernst van een verstoord incident en de potentiële gevolgen te bevatten.

De verantwoordelijke voor het voorgoed oplossen van het incident dient alle acties vast te leggen in het Incidentenlogboek.

#### 4.1.3. Crisismanager

De crisismanager dient de voortgang van de incidentbehandeling te bewaken evenals de periode van versterking van afzonderlijke activiteiten, en de tijd te bepalen die nodig is om het incident op te lossen.

Indien de vereiste tijd om het incident op te lossen langer is dan de recovery time objective van een bepaalde activiteit, dan dient het herstelplan voor een verstoerde activiteit te worden geactiveerd. In dat geval dient de crisismanager alle recovery managers beheerders voor herstel te vertellen die hun herstelplannen zullen moeten gaan activeren.

## 4.2. Beheersen en totaal oplossen van een incident

### 4.2.1. Ontruiming van het gebouw (ongeacht het soort incident)

Het gebouw wordt ontruimd naar de in Lijst van Bedrijfscontinuïteitslocaties aangegeven verzamelpunten, als volgt aangegeven in het Bedrijfscontinuïteitsplan.

Crisismanager	<ul style="list-style-type: none"> <li>• In geval de levens of gezondheid van mensen worden bedreigd, vaardig een ontruimingsopdracht uit</li> <li>• Indien Verzamelpunt 1 niet beschikbaar is, door iemand naar de locatie van Verzamelpunt 2 om die te markeren (geplaatste borden, richtingspijlen, vlaggen, verkeersborden, enz.)</li> <li>• In geval van een kwaadaardige bedreiging (bijv. bommelding), beslis over een nieuw verzamelpunt (Verzamelpunt 2) en stel de verantwoordelijken op de hoogte van het uitvoeren van de ontruiming</li> </ul>
Verantwoordelijken voor de ontruiming	<ul style="list-style-type: none"> <li>• Directe ontruiming naar het verzamelpunt</li> <li>• Controleer of alle ruimten leeg zijn na ontruiming, verlaat de ruimten en sluit de deuren</li> </ul>

**Comment [DK10]:** Dit hoofdstuk levert alleen procedures voor enkele potentiële incidenten - procedures voor andere incidenten die zijn beoordeeld als waarschijnlijk door de risicobeoordeling zouden hier moeten worden toegevoegd.



	<ul style="list-style-type: none"> <li>In geval iemand niet in staat was het gebouw te verlaten, informeer dan [telefoonnummer van hulpdienst]</li> </ul>
Alle werknemers	<ul style="list-style-type: none"> <li>Ontruim in overeenstemming met de ontruimingsplannen van uw gebouw</li> <li>Volg de instructies aangegeven door de verantwoordelijke voor onmiddellijke evacuatie</li> <li>Gebruik geen mobiele telefoon gedurende de ontruiming</li> <li>Wanneer wordt ontruimd, neemt u alleen uw ID-kaart en portemonnee mee, neem geen andere zaken met u mee</li> <li>Ondersteun anderen bij de ontruiming indien ze hulp nodig hebben</li> </ul>
Crisis Management Ondersteunings-team	<ul style="list-style-type: none"> <li>Wanneer mensen zich hebben verzameld op het verzamelpunt, houd dan alle aanwezige en vertrokken personen bij</li> </ul>

#### 4.2.2. Brand

Het gebouw wordt ontruimd in overeenstemming met het ontruimingsplan.

Crisismanager	<ul style="list-style-type: none"> <li>In geval de levens of gezondheid van mensen worden bedreigd, vaardigt de crisismanager een ontruimingsoproep af</li> <li>Hij/zij richt het noodoproep aan de schade te beperken of op te ruimen te veilig te stellen, tenzij dit een risico voor mensen vertegenwoordigt</li> </ul>
---------------	--

#### 4.2.3. Onderbreking van stroomtoevoer

Crisis Management Ondersteunings-team	<ul style="list-style-type: none"> <li>Stel de oorzaak van de onderbreking vast - wordt het veroorzaakt door de bekabeling of door de stroomleverancier</li> </ul>
[functie]	<ul style="list-style-type: none"> <li>Los het probleem gezamenlijk op met de stroomleverancier</li> </ul>
Alle werknemers	<ul style="list-style-type: none"> <li>In overeenstemming met de herstelplannen, vervolg met noodprocedures om de activiteiten af te voeren, zonder het gebruik van elektriciteit</li> </ul>
Werknemers in [IT-afdeling]	<ul style="list-style-type: none"> <li>Bewaak UPS-apparaten en stel indien noodzakelijk een informatiesysteem buiten werking</li> </ul>

#### 4.2.4. Aardbeving

Het gebouw wordt ontruimd in overeenstemming met het ontruimingsplan.

Alle werknemers	<ul style="list-style-type: none"> <li>• Zoek beschutting onder een deurkozijn, dichtbij een dragende binnenmuur of onder een bureau</li> <li>• <del>Vertrouw geen liften</del></li> <li>• <del>Niet met werden naar buiten dan een het eind van de werkdag</del></li> <li>• Wanneer de aardbeving over is, probeer mensenlevens te redden tenzij deze meer schade aan de gewonden toebrengt</li> <li>• In geval opdracht is gegeven tot evacuering, ga te werk volgens het ontruimingsplan</li> </ul>
Continuïteitsmanager	<ul style="list-style-type: none"> <li>• In geval van bedreiging van levens of gezondheid van mensen, vaardig een opdracht tot evacuering van het gebouw af wanneer de werkdag is afgelopen</li> </ul>
Crisis Management Ondersteuningsteam	<ul style="list-style-type: none"> <li>• Stop alle (nuts)voorzieningen - gas, elektriciteit, verwarming, ventilatie, waterlevering</li> <li>• Bewak het gebouw en andere gebouwen</li> </ul>

#### 4.2.5. Dreigbrief

Alle werknemers	<ul style="list-style-type: none"> <li>• Indien u een verdachte brief ontvangt, open deze dan niet, houd het aan de uiteinden vast</li> <li>• <del>Stop het in een lege envelop</del></li> <li>• <del>Waarschuw (Politie)</del></li> <li>• Ga volgens de instructies van [functie] verder</li> </ul>
[functie]	<ul style="list-style-type: none"> <li>• Waarschuw de politie op [telefoonnummer]</li> <li>• <del>Waarschuw de bestuurscommissie van de werknemers die de brief heeft gemaakt</del></li> <li>• Voer de maatregelen uit zoals geïnstrueerd door de politie</li> </ul>

#### 4.2.6. Dreigtelefoontje / bommelding

Alle werknemers	<ul style="list-style-type: none"> <li>• Indien u een dreigtelefoontje ontvangt, schrijf dan de exacte tijd en het <del>telefoonnummer van de beller op</del></li> <li>• <del>Schrijf de exacte woorden van de beller op</del></li> <li>• Sta toe dat de beller zo veel mogelijk zegt, zonder onderbrekingen: <ul style="list-style-type: none"> <li>- probeer hem/haar zoveel mogelijk te laten praten</li> <li>- <del>Verhoor een vragen, mag dat u het niet begrijpt wilt u zeggen</del></li> <li>- <del>Indien uw telefoon afgevoerd is met een telefoonhoorn, zet het telefoongesprek dan op de luidspreker en vraag iemand vertalingen te maken</del></li> <li>- <del>Verhoor alle verzoek geboden door de beller</del></li> </ul> </li> <li>• In geval van een bommelding, stel de beller dan de volgende vragen: <ul style="list-style-type: none"> <li>- Wanneer gaat de bom af? Wanneer?</li> <li>- <del>Niet het worden gebelust? Hoe?</del></li> <li>- Waar is het geplaatst?</li> </ul> </li> </ul>
-----------------	--

	<ul style="list-style-type: none"> <li>- Hoe ziet het ding eruit?</li> <li>- Waarom is het geïncideerd: wat zijn de oorzaken?</li> <li>- Wie belt er? Kun je zichzelf aanmelden?</li> </ul> <ul style="list-style-type: none"> <li>• Open alleen de kantoorduren indien u er zeker van bent dat ze niet zijn verboden met de baan</li> <li>• Zoek het gebouw niet op maar de baan! Dit is de taak van de politie</li> <li>• Raak geen onbekende objecten aan</li> <li>• Indien een evacuering is uitgesproken, handel dan volgens het ontruimingsplan</li> </ul>
Crisismanager	<ul style="list-style-type: none"> <li>• Waarschuw de verantwoordelijke in de organisatie-eenheid waaraan de dreiging is gericht</li> <li>• Gaafde met de standaard verzamelpunten – selecteer een nieuw verzamelpunt</li> <li>• Indien u weet dat de baan niet zal afgaan, waarbij een evacuering uit, verzamelpunt dient minstens 300 meter verderop te zijn</li> <li>• Breng de verantwoordelijken voor ontruiming en het Crisis Management (ondersteuningsteam) op de hoogte van de locatie van het nieuwe verzamelpunt</li> <li>• In geval van explosie, besluit dan dat de gewonden zo snel mogelijk van het getroffen gebied worden weggevoerd</li> </ul>

#### 4.2.7. Uitval telecommunicatie

Werknemers [IT-afdeling]	<ul style="list-style-type: none"> <li>• Een werknemer ontvangt informatie van de uitval</li> <li>• Wanneer nodig, wordt contactloos met de leveranciers van IT-diensten</li> </ul>
Werknemers - gebruikers van communicatie diensten	<ul style="list-style-type: none"> <li>• Gebruik alternatieve middelen van communicatie</li> </ul>

#### 4.2.8. Uitval informatiesysteem

Werknemers [IT-afdeling]	<ul style="list-style-type: none"> <li>• Een werknemer ontvangt informatie over het incident</li> <li>• Wanneer nodig, wordt contactloos met de leveranciers van IT-diensten</li> <li>• Neem noodzakelijke maatregelen om het incident met betrekking tot het informatiesysteem te voorkomen of te beheersen</li> </ul>
Crisismanager	<ul style="list-style-type: none"> <li>• Raadplegen van alle relevante diensten, beoordeling van de ernst van het incident</li> </ul>
Alle werknemers	<ul style="list-style-type: none"> <li>• Via, indien mogelijk, verder met noodprocedures om de activiteiten uit te voeren</li> </ul>

**4.2.9. Virusaanval**

Werknemers [IT afdeling]	<ul style="list-style-type: none"> <li>Een werknemer ontvangt informatie over het incident</li> <li>Indien te maken met een onbekend type virus (kwaadaardige code), dient de leveringsinformatie van de leverancier van de software te worden gewaarschuwd</li> <li>Waarschuw de producent van de antivirussoftware</li> <li>Indien de externe leverancier van het virus is geïdentificeerd, neem dan contact op met de leverancier van de organisatie van IT verantwoordelijke</li> <li>Coördineer alarmering van andere werknemers, speciaal die berichten ontvangen met het geïdentificeerde</li> <li>Wanneer nodig, coördineer het proces met de leveranciers van IT-diensten</li> </ul>
Alle werknemers	<ul style="list-style-type: none"> <li>Koppel elke geïnfecteerde PC fysiek los van het netwerk; stel het draadloze netwerk buiten werking, Bluetooth, etc.</li> <li>Stel geen netwerkapparaten en servers buiten werking – dit is de taak van de mensen van de [IT afdeling]</li> </ul>
Werknemers [IT afdeling]	<ul style="list-style-type: none"> <li>Indien de computer nog steeds niet losgekoppeld is van het netwerk, bevestig dat het netwerk wordt hersteld</li> <li>Stel alle draadloze verbindingen op de computer buiten werking</li> <li>Sluit uw software af (inclusief het operating systeem) - voor servers, bevestig dat de gebruikers van het systeem hiervan worden gewaarschuwd</li> <li>Zoek informatie over de soort kwaadaardige code en neem de noodzakelijke stappen voor de afsluiting ervan (van het internet, van de leverancier)</li> <li>Handel vervolgens volgens de ontvangen instructies</li> </ul>

**4.2.10. Overtreding van de interne of externe regels**

[functie]	<ul style="list-style-type: none"> <li>De procedure wordt uitgevoerd als vereist in de arbeidswetten die de discipline proceduren regelen en de discipline regels van de eigen organisatie</li> </ul>
-----------	---

**5. Registratiebeheer op basis van dit document**

Naam registratie	Opslaglocatie	Persoon verantwoordelijk voor opslag	Beveiligingsmaatregelen voor registraties	Bewaartermijn
Incidentenlogboek	Gedeelde map op het internet	[functie]	alleen [functie] heeft het recht om de lijst te bewerken	3 jaar



Alleen [functie] kan andere werknemers toegang tot de registraties verlenen.

### 6. Geldigheid en documentbeheer

Dit document is geldig vanaf [datum].

Dit document, samen met alle andere materialen, wordt opgeslagen op de volgende manier:

- de papieren vorm van de documenten worden op de volgende locaties opgeslagen:  
Commandocentrum, en alle afdelingen waar activiteiten
- de elektronische vorm van het document wordt opgeslagen op de volgende wijze: [geef de naam van de map op het intranet]

De eigenaar van dit document is [functie]. (12/15) Alleen het document te controleren en indien nodig het minstens eens per jaar bij te werken.

Wanneer de doeltreffendheid en toereikendheid van dit document wordt beoordeeld, dan dienen de volgende criteria in ogenschouw te worden genomen:

- aanpak incidenten die niet worden gelinkt door dit document
- of de in dit document beschreven stappen voldoende zijn in werkelijke situaties
- reactietijd op incident

[functie]

[naam]

[handtekening]

**Comment [DK11]:** Sla het document op om alleen toegang voor geautoriseerde personen mogelijk te maken.

**Comment [DK12]:** T Dit is slechts een aanbeveling, pas de frequentie zo nodig aan.

**Comment [DK13]:** Alleen noodzakelijk indien de Procedure voor Beheersing voor Documenten en Registraties een ondertekening voorschrijft.