Bijlage 1 – Incidentenopvangplan

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, danvindt 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

Versieblad

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

INHOUDSOPGAVE

1. Doel, toepassingsgebied en gebruikers

Het doel van dit Plan is om de bescherming van de gezondheid of veiligheid van mensen in geval van [illegible]

Dit Plan is van toepassing op alle grote incidenten die enige activiteit binnen het ISMS [BCMS] [illegible] 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	[illegible]
Elke werknemer	De verantwoordelijke organisatie-eenheid waarschuwen over het incident
[functie] of werknemer in [naam van organisatie-eenheid]	[illegible] gerelateerde incidenten op te lossen
[[functie] of werknemer in [naam van organisatie-eenheid]	Alle stappen noodzakelijk om alle andere incidenten op te lossen
[functie]	[illegible]
[functie]	Communicatie met de publieke media – deze persoon heeft als enige de [illegible]
[functie]	Psychische hulp voor werknemers

Comment [DK2]: Dient de in het [illegible]

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

3. Communicatie

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

De volgende tabel vermeldt de verantwoordelijkheden voor communicatie (zowel sturen als ook het [illegible] partijen:

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

Comment [DK5]: Neem de [illegible] 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 [illegible] verantwoordelijke zoals aangegeven in de vorige tabel.
2. Een verantwoordelijke moet het eens zijn met [functie] over de inhoud van de communicatie
3. [illegible] goedgekeurd door [functie] voor dat dergelijke informatie wordt vrijgegeven
4. Na de verkregen toestemming, levert de verantwoordelijke de informatie aan de [illegible].

De verantwoordelijke genoemd in de vorige tabel is verantwoordelijk voor het vastleggen van elke [illegible].

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

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 [illegible]
- [illegible] eenheid]

Comment [DK8]: Indien het karakter van het [illegible] e-mail of door middel van een softwaretool.

Enig andere gebeurtenis of systeemkwetsbaarheid dat zich nog niet tot een verstorend incident heeft [illegible]

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 [illegible].

In geval date en incident optreedt, dan kunnen werknemers alleen vrijuit spreken met hun [illegible] crisismanager wordt overgelaten.

4.1.2. Omgaan met een verstorend incident

De persoon die de informatie over een verstorend incident heft ontvangen dient te beoordelen of [illegible] 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 [illegible]
- [illegible] verantwoordelijkheden
- breng [functie] op de hoogte, die moet overwegen of enig belangenpartij dient te worden gewaarschuwd
- [illegible] 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 [illegible]

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 [illegible] lossen.

Indien de vereiste tijd om het incident op te lossen langer is dan de recovery time objective van een [illegible] hun herstelplannen zullen moeten gaan activeren.

4.2. Beheersen en totaal oplossen van een incident

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

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

Het gebouw wordt ontruimd naar de in Lijst van Bedrijfscontinuïteitslocaties aangegeven [illegible]

Crisismanager	• In geval de levens of gezondheid van mensen worden bedreigd, vaardig een ontruimingsopdracht uit • [illegible] richtingspijlen, vlaggen, verkeersborden, enz.) • In geval van een kwaadaardige bedreiging (bijv. bommelding), beslis over [illegible] op de hoogte van het uitvoeren van de ontruiming
[illegible] voor de ontruiming	• Directe ontruiming naar het verzamelpunt • [illegible] verlaat de ruimten en sluit de deuren

	• In geval iemand niet in staat was het gebouw te verlaten, informeer dan [telefoonnummer van hulpdienst]
[illegible]	• Ontruim in overeenstemming met de ontruimingsplannen van uw gebouw • [illegible] onmiddellijke evacuatie • Gebruik geen mobiele telefoon gedurende de ontruiming • [illegible] mee, neem geen andere zaken met u mee • Ondersteun anderen bij de ontruiming indien ze hulp nodig hebben
Crisis Management Ondersteunings-team	• Wanneer mensen zich hebben verzameld op het verzamelpunt, houd dan [illegible]

4.2.2. Brand

Het gebouw wordt ontruimd in overeenstemming met het ontruimingsplan.

Crisismanager	• In geval de levens of gezondheid van mensen worden bedreigd, vaardigt de [illegible] • [illegible] veilig te stellen, tenzij dit een risico voor mensen vertegenwoordigt

4.2.3. Onderbreking van stroomtoevoer

Crisis Management Ondersteunings-team	• Stel de oorzaak van de onderbreking vast - wordt het veroorzaakt door de bekabeling of door de stroomleverancier
[functie]	• Los het probleem gezamenlijk op met de stroomleverancier
[illegible]	• In overeenstemming met de herstelplannen, vervolg met noodprocedures [illegible]
Werknemers in [IT-afdeling]	• Bewaak UPS-apparaten en stel indien noodzakelijk een informatiesysteem buiten werking

4.2.4. Aardbeving

[illegible] met het ontruimingsplan.

Alle werknemers	• Zoek beschutting onder een deurkozijn, dichtbij een dragende binnenmuur of onder een bureau • [illegible] • [illegible] • Wanneer de aardbeving over is, probeer mensenlevens te redden tenzij deze [illegible] • [illegible] ontruimingsplan
[illegible]	• In geval van bedreiging van levens of gezondheid van mensen, vaardig een [illegible] afgelopen
Crisis Management Ondersteuning-team	• Stop alle (nuts)voorzieningen - gas, elektriciteit, verwarming, ventilatie, [illegible] • [illegible]

4.2.5. Dreigbrief

[illegible]	• Indien u een verdachte brief ontvangt, open deze dan niet, houd het aan de uiteinden vast • [illegible] • [illegible] • Ga volgens de instructies van [functie] verder
[functie]	• Waarschuw de politie op [telefoonnummer] • [illegible] • Voer de maatregelen uit zoals geïnstrueerd door de politie

4.2.6. Dreigtelefoontje / bommelding

Alle werknemers	• Indien u een dreigtelefoontje ontvangt, schrijf dan de exacte tijd en het [illegible] • [illegible] • Sta toe dat de beller zo veel mogelijk zegt, zonder onderbrekingen: - probeer hem/haar zoveel mogelijk te laten praten - [illegible] - [illegible] telefoongesprek dan op de luidspreker en vraag iemand [illegible] - [illegible] • In geval van een bommelding, stel de beller dan de volgende vragen: - Wanneer gaat de bom af? Wanneer? - [illegible] - Waar is het geplaatst?

	- Hoe ziet het ding eruit? - [illegible] - [illegible] • Open alleen de kantoordeuren indien u er zeker van bent dat ze niet zijn [illegible] • [illegible] • Raak geen onbekende objecten aan • [illegible] ontruimingsplan
Crisismanager	• Waarschuw de verantwoordelijke in de organisatie-eenheid waaraan de dreiging is gericht • [illegible] • [illegible] verzamelpunt dient minstens 300 meter verderop te zijn • Breng de verantwoordelijken voor ontruiming en het Crisis Management [illegible] verzamelpunt • In geval van explosie, besluit dan dat de gewonden zo snel mogelijk van het [illegible]

4.2.7. Uitval telecommunicatie

Werknemers [IT-afdeling]	• Een werknemer ontvangt informatie van de uitval • [illegible] met de leveranciers van IT-diensten
[illegible]	• Gebruik alternatieve middelen van communicatie

4.2.8. Uitval informatiesysteem

Werknemers [IT-afdeling]	• [illegible] • [illegible] diensten • Neem noodzakelijke maatregelen om het incident met betrekking tot het [illegible]
[illegible]	• Raadplegen van alle relevante diensten, beoordeling van de ernst van het incident
Alle werknemers	• [illegible] voeren

4.2.9. Virusaanval

[illegible]	• Een werknemer ontvangt informatie over het incident • Indien te maken meet een onbekend type virus (kwaadaardige code), dient de [voor informatiebeveiliging verantwoordelijke van naam organisatie] te worden gewaarschuwd • Waarschuw de producent van de antivirussoftware • Indien de externe bron van het virus is geïdentificeerd, neem dan contact op met de in de organisatie voor IT verantwoordelijke • Coördineer alarmering van andere werknemers, speciaal die berichten uitwisselen met het geïnfecteerde • Wanneer nodig, coördineer het proces met de leveranciers van IT-diensten
Alle werknemers	• Koppel elke geïnfecteerde PC fysiek los van het netwerk; stel het draadloze netwerken buiten werking, bluetooth, enz. • Stel geen netwerkapparaten en servers buiten werking – dit is de taak van de mensen van de [IT afdeling]
[illegible]	• Indien de computer nog steeds niet losgekoppeld is van het netwerk, beoordeel indien loskoppeling verdere besmetting voorkomt • Stel alle draadloze verbindingen op de computer buiten werking • Sluit uw software af (inclusief het operating systeem) - voor servers, beoordeel eerst de gebruikers van het systeem moeten worden gewaarschuwd • Zoek informatie over de soort kwaadaardige code en neem de noodzakelijke stappen voor de uitroeiing ervan (van het internet, van de leveranciers) • Handel vervolgens volgens de ontvangen instructies

4.2.10. Overtreding van de interne of externe regels

[functie]	• De procedure wordt uitgevoerd als vereist in de arbeidswetten die de disciplinaire procedures regelen en de disciplinaire regels van de eigen organisatie

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: [illegible]
- [illegible] [geef de naam van de map op het intranet]

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

De eigenaar van dit document is [functie]. [illegible] het minstens eens per jaar bij te werken.

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

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

- [illegible]
- [illegible] zijn in werkelijke situaties
- reactietijd op incident

[functie]

[naam]

_____

[handtekening]

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