Incident   
Response Plan

Incident   
Response Plan

Documentgeschiedenis

Geschiedenis wijzigingen

|  |  |  |  |
| --- | --- | --- | --- |
| Versie | Datum | Gewijzigd door | Omschrijving van de wijzigingen |
| xxx | xxx | xxx | xxx |
| … |  |  |  |

Geschiedenis goedkeuringen

|  |  |  |
| --- | --- | --- |
| Naam | Functie | Datum goedkeuring |
| xxx | xxx | xxx |
| … |  |  |

Dit document geldt vanaf **[date]**.

Dit document wordt als volgt bewaard:

* In papieren vorm op volgende locaties: **[lijst locaties]**.
* In digitale vorm op volgende locaties: **[locatie op bv. intranet]**.

Eigenaar van dit document is **[functie]**. Hij checkt minstens 1 maal per jaar of updates nodig zijn.

INHOUDSTAFEL

[Documentgeschiedenis 2](#_Toc58004200)

[Geschiedenis wijzigingen 2](#_Toc58004201)

[Geschiedenis goedkeuringen 2](#_Toc58004202)

[Hoofdstuk I. Doel van het document 4](#_Toc58004203)

[Hoofdstuk II. Verband tussen procedures 5](#_Toc58004204)

[Hoofdstuk III. Rollen 8](#_Toc58004205)

[3.1 Helpdesk 8](#_Toc58004206)

[3.2 Incident management team 8](#_Toc58004207)

[3.3 Business continuity team 9](#_Toc58004208)

[3.4 Crisis management team 9](#_Toc58004209)

[Hoofdstuk IV. INCIDENT RESPONSE PLAN 10](#_Toc58004210)

[4.1 Stap 1: Voorbereiding 11](#_Toc58004211)

[4.2 Stap 2: Melding en identificatie 11](#_Toc58004212)

[4.3 Stap 3: Activatie en behandeling 13](#_Toc58004217)

[4.4 Stap 4: Eradication 14](#_Toc58004218)

[4.5 Stap 5: Deactivering 14](#_Toc58004219)

[4.6 Stap 6: Geleerde lessen (post incident review) 15](#_Toc58004220)

[Hoofdstuk V Bijlagen 19](#_Toc58004221)

[5.1. Bijlage 1. Lijst van contacten 19](#_Toc58004222)

[a) Intern 19](#_Toc58004223)

[b) Extern (leveranciers, klanten,…) 21](#_Toc58004224)

[5.2 Bijlage 2. Nuttige documenten 21](#_Toc58004225)

# Hoofdstuk I. Doel van het document

**Het voornaamste doel** van het Incident Response Plan is om vooraf te bepalen hoe uw onderneming incidenten zal aanpakken om eventuele schade en risico’s te beperken en ervoor te zorgen dat het bedrijf zijn essentiële activiteiten kan verder zetten.

Dit incidentbeheerplan legt de organisatie, maatregelen en aanbevolen procedures vast met als doel:

* Een incident herkennen en erop reageren;
* Snel en efficiënt de situatie beoordelen;
* De juiste personen en organisaties informeren;
* De responsactiviteiten van het bedrijf aansturen en het activeren van een commandocentrum;
* De reactie van het bedrijf versnellen op basis van de ernst van het incident;
* Beginnen, indien nodig, om het bedrijf na het incident opnieuw op te starten

Dit plan veronderstelt dat uw bedrijf vooraf reeds een Risk Assessment en een Risk Treatment heeft uitgevoerd.

# Hoofdstuk II. Verband tussen procedures

Het schema hieronder geeft aan hoe het incidentenbeheer past binnen de andere procedures.

**1. Risk Assessment & Risk Treatment**

**2. Business Continuity Plan**

**Belangrijke leveranciers**

**Klanten**

**B**

**A**

**B**

**C**

**D**

**E**

**E**

**F**

**H**

**G**

**G**

**I**

**H**

**J**

**A**

**3. Incidentenbeheer  
IRP  
CMP  
DRP**

1. Om te beschikken over een efficiënt incidentenbeheer, wordt ervan uitgegaan dat het bedrijf de templates voor Risk Assessment en Risk Treatment al heeft afgerond. Het risiconiveau en de waarschijnlijkheid van een incident zijn afhankelijk van het Risk Treatment dat u heeft uitgevoerd. Ook hangt het beheer van een incident sterk af van de preventieve en herstellende maatregelen die u heeft genomen.
2. Bij het opstellen van uw Business Continuity Plan en uw Incident Response Plan is het mogelijk dat u het eerder gemaakte Risk Assessment dient te updaten (zeker wanneer u risico’s probeert bij te stellen door het gebruik van nieuwe tools of door het opstarten van nieuwe projecten).
3. Uw Risk Assessment en uw Business Continuity Plan zullen ook vereisen dat u bepaalde zaken checkt met uw leveranciers, uw contracten nakijkt en hen eventueel bepaalde vereisten op het vlak van serviceniveau (Service Level Agreement SLA) of contractuele clausules oplegt.
4. De continuïteit van de activiteiten van uw bedrijf is sterk gelinkt aan het incidentenbeheer omdat u er moet voor zorgen dat u ook tijdens een incident de (minstens essentiële) activiteiten kan blijven voortzetten. De beheerder van het Business Continuity Plan bezorgt daarom alle nodige informatie aan de verantwoordelijke voor het Incident Response Plan.
5. U kan vaak via uw klanten of leveranciers te weten komen dat een bepaald incident zich voordoet.
6. Het merendeel van de incidenten vraagt niet om het activeren van het Business Continuity Plan, omdat deze ‘kleinere’ incidenten geen reële impact hebben op de activiteiten. Wanneer een incident met impact op uw activiteiten zich voordoet, zal de beheerder van het Incident Response Plan de beheerder van het Business Continuity Plan verwittigen, zodat hij/zij het BCP kan activeren. Gedurende het incident zorgt de beheerder van het Incident Response Plan voor een regelmatige rapportering naar de beheerder van het Business Continuity Plan. Na afloop van het incident, bezorgt hij/zij ook een “Post Incident Review” aan de beheerder van het Business Continuity Plan.
7. Indien het incident geen impact heeft op de bedrijfscontinuïteit, kan de beheerder van het Incident Response Plan, indien nodig, zelf klanten en leveranciers verwittigen in verband met het incident.
8. Indien het incident gevolgen heeft voor de bedrijfscontinuïteit zal de beheerder van het Business Continuity Plan, indien nodig, klanten en leveranciers op de hoogte brengen, in functie van de informatie die hij ontvangt van de functionele diensten en via de beheerder van het Incident Response Plan.
9. Na een incident is het mogelijk dat een Post Incident Review uitwijst dat het Risk Assessment en Risk Treatment bijgestuurd moeten worden.
10. Na een incident is het mogelijk dat een Post Incident Review uitwijst dat contracten met bepaalde leveranciers herzien moeten worden.

Na het beheren van een incident is het mogelijk dat u het bestaande Risk Assessment en Risk Treatment of uw Business Continuity Plan moet verbeteren. **Voor meer informatie over de verschillende procedures, verwijzen we u graag door naar de beschikbare templates.**

Alle personen die betrokken zijn bij het continuïteitsplan van het bedrijf dienen hun concrete rol te kennen en over de meest recente versie van het plan te beschikken. (Denk eraan om deze versie ook op papier te bewaren).

1. De beheerder van het Incident Response Plan (IRP) verwittigt de beheerder van het Crisis Management Plan (CMP) dat er een incident met impact op de continuïteit van het bedrijf aan de gang is of hierover een vermoeden bestaat. De beheerder van het Crisis Management Plan houdt de beheerder van het IRP op de hoogte en kan op hem rekenen voor ondersteuning.
2. De beheerder van het Crisis Management Plan (CMP) verwittigt de beheerder van het Business Continuity Plan (BCP)
3. De beheerder van het Business Continuity Plan (BCP) informeert en adviseert de beheerder van het Crisis Management Plan (CMP)
4. De beheerder van het Crisis Management Plan (CMP) verwittigt de beheerder van het Disaster Recovery Plan (DRP)
5. De beheerder van het Disaster Recovery Plan informeert en adviseert de beheerder van het Crisis Management Plan.
6. De beheerders van het Business Continuity Plan (BCP) en Disaster Recovery Plan (DRP) houden elkaar op de hoogte van de evoluties.
7. De beheerder van het Incident Response Plan (IRP) verwittigt de beheerder van het Business Continuity Plan (BCP) (zonder de beheerder van het Crisis Management Plan te verwittigen). De beheerder van het Business Continuity Plan (BCP) kan vertrouwen op de vaardigheden van het Incident Response Team.

**Incident Response Plan (IRP)**

**Crisis Management Plan (CMP)**

**Disaster Recovery Plan (DRP)**

**Business Continuity Plan (BCP)**

**6**

**7**

**1**

**4**

**5**

2

**3**

Om ervoor te zorgen dat het Business Continuity Plan (BCP) daadwerkelijk functioneert in het geval van een incident is het belangrijk dat de **voorziene procedures vooraf regelmatig en grondig worden getest**. Denk er ten minste eenmaal per jaar en na elk incident, crisis of ramp aan om uw plannen te herbekijken en de "lessons learned" te bepalen zodat u de plannen kan bijsturen in functie van de ervaringen en de noden van uw bedrijf.

# Hoofdstuk III. Rollen

Het gaat erom de verschillende rollen en verantwoordelijkheden duidelijk te omschrijven, zodat iedereen de aan hem/haar toegewezen rol kent.

## 3.1 Helpdesk

Le “helpdesk” of de dienst die verantwoordelijk is voor incidenten, zorgt voor het invoeren van adequate procedures om incidenten te registeren, met behulp van de juiste tools (software)

| **Functie** | **Rollen** |
| --- | --- |
| Teamleider Helpdesk  (Helpsdesk Manager) | * Monitoren van service level agreements (Service Level Agreement SLA) * Indien nodig feedback bezorgen aan de beheerder van het Incident Response Plan |
| Helpdesk medewerker  (Helpdesk Operator) | * Incidenten registeren en prioriteiten toekennen * Incidenten oplossen in 1e lijn, volgens de voorziene procedures * De Helpdesk Manager informeren |
| … |  |

## 3.2 Incident Management Team

Het incident Management Team is verantwoordelijk voor de uitvoering van het plan voor het beheer van alle incidenten met een impact op de bedrijfsprocessen.

| **Functie** | **Rollen** |
| --- | --- |
| Beheerder incident management team  (Incident Response Manager) | * Ontwikkelen en uitvoeren van het Incident Response Plan voor specifieke scenario’s. * Opvolging van lopende incidenten. * De beheerder van het Crisis Management Plan en/of de beheerder van het Business Continuity Plan verwittigen. |
| Leden incidentbeheerteam  (Incident Response Team) | * Kleine en grote incidenten oplossen in 2e of 3e lijn. * Communiceren met teams die kunnen helpen bij het oplossen van incidenten. |
| … |  |

## 3.3 Business Continuity Team

Het Business Continuity Team zorgt voor de uitvoering van het BCP in het geval van een incident dat een impact heeft op de bedrijfsprocessen. De rollen en verantwoordelijkheden van het BCP zijn vastgelegd in het Business Continuity Plan (zie templates)

## 3.4 Crisis Management Team

Het Crisis Management Team zorgt voor het beheer van het Crisis Management Plan en de bijhorende procedures. Zij zijn verantwoordelijk voor de coördinatie en communicatie in geval van een ramp. De rollen en verantwoordelijkheden van het CMT zijn vastgelegd in het Crisis Management Plan (zie templates)

# Hoofdstuk IV. INCIDENT RESPONSE PLAN

Het Incident Response Plan is gebaseerd op 6 fasen :

## 4.1 Stap 1: voorbereiding

Zie ook Risk Assessment en Risk Treatment.

Denk aan de volgende elementen bij het uitwerken van uw incidentbeheersplan:

* Hoe omgaan met een incident (identificeren, inperken, elimineren en de activiteiten hervatten na het incident)
* Bewaken, detecteren, analyseren et signaleren van gebeurtenissen en incidenten
* Registeren van incidenten
* Evalueren en beslissingen nemen
* Hoe kwetsbaarheden in informatiebeveiliging en/of privacybescherming beoordelen
* Incidenten escaleren (naar het Business Continuity Team of het Crisis Management Team)
* Hoe terugkeren naar een normale situatie na het incident?
* Wanneer communiceren, wat communiceren en naar wie

## 4.2 Stap 2: melding en identificatie

Het is essentieel om een incident snel te kunnen opsporen, identificeren en kwalificeren/classificeren om de impact op de continuïteit van de activiteiten te beperken door de juiste procedure te activeren. De persoon die de melding van het incident ontvangt, kwalificeert het incident op van vooraf vastgestelde criteria.

Elke werknemer moet elk incident of gebeurtenis die tot een incident kan leiden, zo snel mogelijk melden. Klanten en leveranciers kunnen ook een incident melden.

Denk eraan middelen te installeren om incidenten te melden.

De persoon die de informatie ontvangt (bv. Helpdesk) dient deze bijvoorbeeld als volgt in te delen:

1. **Zwak** - er hebben zich geen incidenten voorgedaan, maar de gebeurtenis houdt verband met een systeem, proces of organisatie en kan een incident in de nabije of toekomstige toekomst veroorzaken;
2. **Klein** - een incident dat geen significante impact heeft op de bedrijfscontinuïteit;
3. **Groot** - een incident dat een significante impact kan hebben op de organisatie, maar nog niet als een crisis wordt beschouwd;
4. **Crisis** - een incident dat een aanzienlijke impact kan hebben op de organisatie en de bedrijfscontinuïteit.

### 4.2.1. Zwak

Wanneer er informatie rond een zwakte of gebeurtenis wordt gerapporteerd, analyseert de bevoegde medewerker dit, stelt indien mogelijk de oorzaak vaste en stelt indien nodig preventieve of corrigerende maatregelen voor.

### 4.2.2 Klein

Wanneer kleine incidenten worden vastgesteld of gerapporteerd, zal de bevoegde medewerker:

1. Maatregelen nemen om het incident te beheersen;
2. Het incident volgens het gepaste proces rapporteren en de ernst beoordelen rekening houdend met de vastgelegde serviceniveaus en drempels;
3. De oorzaak van het incident analyseren;
4. Corrigerende maatregelen nemen om de oorzaak van het incident weg te nemen (indien mogelijk binnen de afgesproken termijn)
5. Diegenen die door het incident getroffen zijn of erbij betrokken zijn op de hoogte stellen van de oplossing

### 4.2.3. Groot

Wanneer grote incidenten worden vastgesteld of gerapporteerd, zal de bevoegde medewerker:

1. Maatregelen nemen om het incident te beheersen;
2. De ernst evalueren op basis van gedefinieerde serviceniveaus en drempels. Een klein incident kan worden uitgebreid tot een groot incident als de oplostijd de overeengekomen serviceniveaus overschrijdt of als de impact blijft toenemen;
3. Alle belanghebbenden die verantwoordelijk zijn voor het incident dat zich heeft voorgedaan in hun verantwoordelijkheidsgebied informeren en de verwachte oplossingstijd aangeven (zie Business Continuity Plan en Crisisbeheersingsplan);
4. Bij een incident het juiste responsteam samenstellen;
5. De voortgang van het incident bewaken en rapporteren over de voortgang van incidentmanagement;
6. De oorzaak van het incident analyseren;
7. Corrigerende maatregelen nemen om de oorzaak van het incident weg te nemen;
8. Diegenen die door het incident getroffen zijn of erbij betrokken zijn op de hoogte stellen van de oplossing
9. Als het grote incident niet op tijd wordt opgelost, kan het incident leiden tot een crisissituatie volgens de escalatieprocedure zoals beschreven in het Crisis Management Plan.

Indien het incident niet kan opgelost worden binnen de voorzien termijn, zal de beheerder van het incident response team onmiddellijk het Business Continuity Team en/of het Crisis Management Team contacteren, om te kunnen evalueren of het BCP of CMP geactiveerd moeten worden...

| **Actie** | **Functie** | **Links naar andere documenten**  ***Naam en referentie*** |
| --- | --- | --- |
| De crisisbeheerder regelmatig informeren over de situatie en de voorziene oplossingstermijn. | Incident Manager aan de beheerder van het Crisis Management Plan | Crisis Management Plan |
| Regelmatig evalueren van de voorzien oplossingstermijn. Indien deze termijn de vastgelegde Recovery Time Objective (RTO) overschrijdt, moet het incident geëscaleerd worden naar het Business Continuity Team. | Incident Manager aan de beheerder van het Business Continuity Plan | Business Continuity Plan |
| … |  |  |

### 4.2.4. Crisis

In het geval van een crisis dient het Crisis Management Plan geactiveerd te worden. (zie Crisis Management Plan)

**Loggen van incidenten**

**Ongeacht de aard van het incident is het belangrijk om tijdens de gehele duur een logboek bij te houden.**

**De person of personen verantwoordelijk voor het beheer van het incident moeten alle ondernomen acties in dit logboek noteren.**

**Onderstaande tabel kan gebruikt worden als voorbeeld voor een logboek:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Datum** | **Type incident** | **Korte beschrijving van het incident** | **Opvolgend team** | **Gedetailleerde beschrijving (impact, duur, getroffen activiteiten, toegewezen middelen...)** | **Beschrijving van de ondernomen acties** |
| **1** |  |  |  |  |  |  |
| **2** |  |  |  |  |  |  |
| **...** |  |  |  |  |  |  |

## 4.3 Stap 3: Activering en behandeling

Het hoofddoel is om de impact van het incident op de continuïteit van de activiteiten van het bedrijf zo snel mogelijk te verminderen.

Tickets worden in het geval van incidenten behandeld door het incident response team. De teamleider houdt toezicht op alle tickets. De volgende acties moeten worden ondernomen om een incident op te lossen:

| **Actie** | **Functie** | **Links naar andere documenten**  ***Naam en referentie*** |
| --- | --- | --- |
| Uitvoeren van een snelle analyse van de situatie op basis van de beschikbare informatie | Helpdesk medewerker |  |
| Bepalen welke acties ondernomen moeten worden om het minimaal toegestane niveau van functioneren te herstellen | Beheerder van het Helpdesk team |  |
| Het incident rapporteren naargelang de ernst ervan | Beheerder van het Helpdesk team aan de beheerder van het Incident Response Team |  |
| Uitvoeren van de te ondernemen acties | Incident response team |  |
| … |  | Zie ook procedures Business Continuity Plan en Crisis Management Plan |

## 4.4 Stap 4: Eradication

Het is niet altijd mogelijk om de oorzaken van het incident tijdens het incident zelf vast te stellen. In dit geval moeten eerst de gevolgen (impact op de bedrijfscontinuïteit) worden aangepakt voordat de oorzaak kan worden vastgesteld. Er moeten echter redelijke inspanningen worden geleverd om de oorzaak te achterhalen en het risico te beperken dat een dergelijk incident zich opnieuw voordoet.

## 4.5 Stap 5: Deactivering

Wanneer de diensten die door een incident werden getroffen, weer normaal functioneren, kan het incident worden afgesloten door het team dat het incident opvolgde (bv. helpdesk) in overeenstemming met de beheerder van het Business Continuity Plan en/of Crisis Management Plan

Het Incident Response Plan wordt gedeactiveerd en er wordt een "Post Incident Review" uitgevoerd (zie stap 6).

De volgende acties moeten worden ondernomen:

| **Actie** | **Functie** | **Links naar andere documenten**  ***Naam en referentie*** |
| --- | --- | --- |
| Afsluiten van het incidententicket | Helpdesk na akkoord van de beheerder van het Incident Respons Plan | Ticket in het kader van incidentenbeheer |
| Deactiveren Incident Response Plan | Beheerder Incident Response Plan |  |
| Post Incident Review | Beheerder Incident Response Plan | Post Incident Review (document) |
| … |  |  |

## 4.6 Stap 6: Geleerde lessen (Post Incident Review)

Het doel is om te leren van haar ervaring door het uitvoeren van een "post incident review" om het incident management in een continu proces te verbeteren.

De Post Incident Review moet ten minste de volgende elementen bevatten:

| **Element** | **informatie** |
| --- | --- |
| **Administratie** |  |
| Incidentnummer in het incidentlogboek: |  |
| Datum en tijd waarop het incident werd vastgesteld: |  |
| Datum en tijd waarop het incident werd opgelost: |  |
| Type incident: |  |
| Ernst van het incident: |  |
| Was er impact voor klanten: |  |
| Wie was beheerder van het incident: |  |
| Beschrijving van het incident: |  |
| ... |  |

|  |  |
| --- | --- |
| **Detectie** |  |
| Wie stelde het incident vast en hoe: |  |
| Werd het incident tijdig opgemerkt of had het eerder ontdekt kunnen worden: |  |
| Kunnen procedures of tools helpen om dit soort incidenten nog vroeger op te sporen: |  |
| Werden de juiste meldingsprocedures gevolgd: |  |
| ... |  |

|  |  |
| --- | --- |
| **Beoordelingen en acties** |  |
| Werd het incident correct ingeschat: |  |
| Was de hiervoor nodige informatie beschikbaar: |  |
| Welke plannen werden geactiveerd (BCP, CMP, DRP): |  |
| Werd het crisisbeheersplan geactiveerd (CMP): |  |
| Welke andere acties werden ondernomen om het incident op te lossen: |  |
| Welke resources werden gebruikt om het incident te beheren: |  |
| Is het plan flexibel genoeg om met onvoorziene events om te kunnen gaan: |  |
| Werden de acties tijdig ondernomen: |  |
| … |  |

|  |  |
| --- | --- |
| **Communicatie** |  |
| Werd er (tijdig) intern gecommuniceerd: |  |
| Werd er (tijdig) extern gecommuniceerd: |  |
| Welke communicatiekanalen werden ingezet: |  |
| Wanneer werd de eerste communicatie uitgestuurd en hoe regelmatig werd deze geüpdatet: |  |
| Werden de juiste personen betrokken: |  |
| Welke communicatie was nuttig: |  |
| Welke communicatie bleek inefficiënt: |  |
| … |  |

|  |  |
| --- | --- |
| **Analyse van de oorzaak** |  |
| Werd de oorzaak van het incident vastgesteld: |  |
| Zijn er verwante of soortgelijke incidenten vastgesteld: |  |
| Is er een onderliggend probleem: |  |
| Is er extra actie nodig om het onderliggende probleem te identificeren (zie stap 4 Eradication): |  |
| ... |  |

|  |  |
| --- | --- |
| **Preventie** |  |
| Wat kunnen we leren uit de gebeurtenis: |  |
| Hoe kunnen we vermijden dat een soortgelijk incident zich opnieuw voordoet, en wie moet hiervoor actie ondernemen: |  |
| ... |  |

|  |  |
| --- | --- |
| **Gepastheid van de reactie** |  |
| Effectieve hersteltijd (vergelijk met Recovery Time Objective – RTO)  Het incident werd binnen de vooropgestelde tijd opgelost:  Voor geen van de activiteiten  Slechts voor enkele activiteiten  Voor alle activiteiten |  |
| Moeten er contracten aangepast worden: |  |
| … |  |

|  |  |
| --- | --- |
| **Heeft het management gepast gereageerd op het incident, zoals voorzien in het Incident Response Plan:** |  |
| Management reageerde niet of onvoldoende |  |
| Management reageerde, maar volgde de plannen niet volledig |  |
| Management reageerde volledig volgens de plannen |  |
| … |  |

|  |  |
| --- | --- |
| **Mate waarin het personeel voorbereid was op het incident:** |  |
| 1. Onvoorbereid |  |
| 2. Deels voorbereid |  |
| 3. Volledig voorbereid |  |
| … |  |

|  |  |
| --- | --- |
| **Gewenste verbeteringen** |  |
| Wat zou kunnen bijgestuurd worden om het incident in de toekomst sneller op te lossen: |  |
| ... |  |

|  |  |
| --- | --- |
| **Schadeclaims** |  |
| Zijn er schadeclaims: |  |
| Werden schadeclaims ingediend bij derden in verband met dit incident: |  |
| … |  |

|  |  |
| --- | --- |
| **Varia** |  |
| … |  |

# Hoofdstuk V Bijlagen

## 5.1. Bijlage 1. Lijst van contacten

### A) Intern

| Rol | Voornaam en NAAM | Functie | Contactgegevens  Probeer steeds 2 contacten per rol te verzamelen, (1 hoofdcontact en 1 in geval van ziekte, vakantie, vertrek van het hoofdcontact) |
| --- | --- | --- | --- |
| Leider van het Business Continuity Team of beheerder van het Business Continuity Plan |  |  | Hoofdcontact:  @  T  M  Andere  @  T  M |
| Leden van het Business Continuity team |  |  | Hoofdcontact:  @  T  M  Andere  @  T  M |
| Interne afdeling 1 |  | Essentiële activiteiten (definieer) | Hoofdcontact:  @  T  M  Andere  @  T  M |
| Interne afdeling 2 |  | Essentiële activiteiten (definieer) | Hoofdcontact:  @  T  M  Andere  @  T  M |

### B) Extern (leveranciers, klanten,…)

| Rol | Voornaam en NAAM | Functie | Contactgegevens  Probeer steeds 2 contacten per rol te verzamelen, (1 hoofdcontact en 1 in geval van ziekte, vakantie, vertrek van het hoofdcontact) |
| --- | --- | --- | --- |
| Leverancier 1 |  |  | Hoofdcontact:  @  T  M  Andere  @  T  M |
| Klant 1 |  |  | Hoofdcontact:  @  T  M  Andere  @  T  M |
| ... |  |  |  |

## 5.2 Bijlage 2. Nuttige documenten

* Risk Assessment en Risk Treatment
* Business Continuity Plan
* Crisis Management Plan