DISASTER RECOVERY PLAN

DISASTER RECOVERY PLAN

Documentgeschiedenis

Geschiedenis wijzigingen

|  |  |  |  |
| --- | --- | --- | --- |
| Versie | Datum | Gewijzigd door | Omschrijving van de wijzigingen (V+1) |
| 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](#_Toc57995441)

[Geschiedenis wijzigingen 2](#_Toc57995442)

[Geschiedenis goedkeuringen 2](#_Toc57995443)

[Inhoudstafel 3](#_Toc57995444)

[Hoofdstuk I. Doel van het document 4](#_Toc57995445)

[Hoofdstuk II. DISASTER RECOVERY PLAN (DRP) 5](#_Toc57995446)

[2.1 Toepassingsgebied van het Disaster Recovery Plan (DRP) 5](#_Toc57995447)

[2.2 Activering van het plan 8](#_Toc57995448)

[2.3 Rollen en verantwoordelijkheden 8](#_Toc57995449)

[2.3.1 Disaster Recovery Team 8](#_Toc57995450)

2.3.2 [Andere interne teams 9](#_Toc57995451)

[Hoofdstuk III Bijlagen 11](#_Toc57995452)

[3.1 Bijlage 1 – Lijst van contacten 11](#_Toc57995453)

[3.1.1 Intern 11](#_Toc57995454)

[3.1.2 Extern (Leveranciers, klanten) 13](#_Toc57995455)

[3.2 Bijlage 2 - Nuttige documenten 14](#_Toc57995456)

# Hoofdstuk I. Doel van het document

**Het voornaamste doel** van een Disaster Recovery Plan is het herstellen van de elementen van de IT-infrastructuur om ervoor te zorgen dat de essentiële diensten van het bedrijf opnieuw in werking kunnen worden gesteld, zoals voorzien in het Business Continuity Plan (zie template)

**Het betreft m.n.:**

* De impact van grote (catastrofale) incidenten op de belangrijkste bedrijfsprocessen definiëren, die bijvoorbeeld de gehele IT-infrastructuur van het bedrijf treffen of essentiële onderdelen ervan.
* Gedocumenteerde herstelprocessen en -procedures opstellen waarmee de IT-infrastructuur hersteld kan worden binnen een vooraf bepaald tijdsbestek (RTO of Recovery Time Objective), conform het Risk assessment en het Business Continuity Plan van het bedrijf.
* Bepalen welke middelen en actoren nodig zijn voor de uitvoering van het Disaster Recovery Plan
* Ervoor zorgen dat het betrokken personeel gesensibiliseerd wordt rond het Disaster Recovery Plan en dat dit DRP up-to-date blijft, in functie van wijzigingen aan de IT-infrastructuur of de verwachtingen van het bedrijf.
* Het Disaster Recovery Plan regelmatig testen. Om ervoor te zorgen dat het plan werkt, is het belangrijk dat de geplande procedures en responstijden regelmatig worden getest en ingeoefend. Alle betrokken bij dit plan moeten hun specifieke rol kennen.

Verwijs indien van toepassing ook naar de in contracten afgesproken servicelevels (SLA) met betrekking tot de IT-infrastructuur om een realistische inschatting te hebben van de hersteltijden.

Hoofdstuk II.  
DISASTER RECOVERY PLAN (DRP)

***“Een plan dat op een plank slaapt, is het papier waarop het is gedrukt niet waard*”**

Om ervoor te zorgen dat dit plan effectief is en dat de IT-infrastructuur binnen de vastgestelde Recovery Time Objectives hersteld kan worden, (zie Risk Assessment en Business Continuity Plan), is het noodzakelijk om het Disaster recovery team goed voor te bereiden, testen en sensibiliseren.

Alle betrokken bij dit plan moeten hun rol kennen.

## 2.1 Toepassingsgebied van het Disaster Recovery Plan (DRP)

Voeg indien mogelijke een schematische weergave van uw IT-infrastructuur toe in bijlage. Het kan ook nuttig zijn om te specifiëren wat NIET binnen het toepassingsgebied van het Disaster Recovery Plan valt, om eventuele twijfels weg te nemen.

Onderstaande elementen van de IT-infrastructuur vallen onder dit plan:

| **INFRASTRUCTUUR IN DE DATACENTERS** | | | | |
| --- | --- | --- | --- | --- |
| **Lokalisatie** | **Type** | **Component** | **Beschrijving van de belangrijkste processen**  Bv: verhoudingen tussen componenten, impact in geval van vermindering of onderbreking van de activiteit (zie Risk Assessment) … | **Recovery Time Objectives (RTO)**  Zie Risk Assessment en Business Continuity Plan  (Check ook contracten met externe partijen) |
| Datacenter A |  |  |  |  |
|  | Servers |  |  | Bv: 15 min, 4u.… |
|  | servers |  |  |  |
|  | ... |  |  |  |
|  | Switch |  |  |  |
|  | Switch |  |  |  |
|  | ... |  |  |  |
|  | Verbinding |  |  |  |
|  | Verbinding |  |  |  |
|  | ... |  |  |  |
| Datacenter B |  |  |  |  |
|  | Servers |  |  |  |
|  | Servers |  |  |  |
|  | ... |  |  |  |
|  | Switch |  |  |  |
|  | Switch |  |  |  |
|  | ... |  |  |  |
|  | Verbinding |  |  |  |
|  | Verbinding |  |  |  |
|  | ... |  |  |  |

| **INFRASTRUCTUUR BUITEN DE DATACENTERS** | | | | |
| --- | --- | --- | --- | --- |
| **Lokalisatie** | **Type** | **Component** | **Beschrijving van de belangrijkste processen**  Bv: verhoudingen tussen componenten, impact in geval van vermindering of onderbreking van de activiteit (zie Risk Assessment) … | **Recovery Time Objectives (RTO)**  Zie Risk Assessment en Business Continuity Plan  (Check ook contracten met externe partijen) |
|  | Core component (ATM—Asynchronous Transfer Mode) |  |  |  |
|  | Core component (IP – Internet Protocol) |  |  |  |
|  | Core component (DWDM – Dense Wavelength Division Multiplexing) |  |  |  |
|  | Core component (SONET – Synchronous Optical NETwork) |  |  |  |
|  | Core component (...) |  |  |  |
|  | … |  |  |  |
|  | RAN (Radio Access Network) component |  |  |  |
|  | RAN component |  |  |  |
|  | ... |  |  |  |

## 2.2 Activering van het plan

Het Disaster Recovery Plan kan worden geactiveerd om ernstige incidenten of crisissituaties aan te pakken die invloed hebben op de IT-infrastructuur. Het activeren van het plan kan gebeuren op vraag van:

* De beheerder van het Business Continuity Plan (leider van het Business Continuity Team)
* De beheerder van het Crisis Managent Plan (leider van het Crisis Management Team)
* De IT-verantwoordelijke of de directie

Het Disaster Recovery Plan wordt geactiveerd door contact op te nemen met de beheerder (of teamleider) van het Disaster Recovery Plan. De beheerder van het DRP communiceert vervolgens met de beheerder van het Business Continuity Plan en de beheerder van het Crisis Management Plan en start indien van toepassing de herstelprocedure op.

In tijden van “nood” zullen niet alle activiteiten aan 100% kunnen draaien. Het doel is om het economische voortbestaan van het bedrijf te verzekeren totdat het zich kan herorganiseren of een aanvaardbare oplossing kan vinden om de geleden ramp op te vangen.

## 2.3 Rollen en verantwoordelijkheden

Het gaat erom rollen en verantwoordelijkheden vast te leggen voor de uitvoering van de verschillende activiteiten.

### 2.3.1 Disaster Recovery Team

Het Disaster Recovery Team is verantwoordelijk voor de acties gelinkt aan het activeren van het Disaster Recovery Plan.

* De beheerder (leider van het team) van het Disaster Recovery Team:
* Stelt het Disaster Recovery Plan op
* Stuurt de uitvoering van het Disaster Recovery Plan aan
* Volgt de voortgang en brengt gedurende de hele ramp verslag uit aan het Business Continuity Team en /of het Crisis Management Team
* ...
* Leden van het Disaster Recovery Team :
* Helpen de leider van het Disaster Recovery Team
* Ondernemen actie zoals voorzien in het Disaster Recovery Plan
* Documenteren hun handelingen en stellen deze documentatie ter beschikking van de beheerder
* ...

### 2.3.2 Andere interne teams

Het Disaster Recovery Team wordt verondersteld samen te werken met :

* Het Business Continuity Team

Het Business Continuity Team is verantwoordelijk voor de bedrijfscontinuïteitsplannen en de uitvoering ervan in geval van ernstige incidenten die de bedrijfsprocessen kunnen beïnvloeden. Het doel is om het hoofd te bieden aan grote incidenten en de gevolgen ervan. De rollen en verantwoordelijkheden van het Business Continuity team zijn vastgelegd in het Business Continuity Plan.

* Het Crisis Management Team

Het Crisis Management Team is verantwoordelijk voor alle procedures voor crisismanagement. De rollen en verantwoordelijkheden van het Crisis Management team zijn vastgelegd in het Crisis Management Plan.

Het Disaster Recovery Team is afhankelijk van tal van resources voor het herstellen van de IT-infrastructuur. Deze resources kunnen worden onderverdeeld in onderstaande categorieën:

| **Infrastructuur** | **Categorieën** | **Resource** | **opmerkingen** |
| --- | --- | --- | --- |
| IT-infrastructuur: naam, type, componenten  (bv : servers, switches, verbindingen... : zie 2.1 Toepassingsgebied) | Personen |  |  |
|  | bv : uitrollen van de oplossing |
|  | bv : test |
| Installaties, gebouwen en infrastructuur |  |  |
|  |  |
|  |  |
| Informatie en documentatie |  |  |
|  |  |
|  |  |
| Derden |  |  |
|  |  |
|  |  |
| Herstellen van software  (Software restoration) | Personen |  |  |
|  |  |
|  |  |
| Installaties, gebouwen en infrastructuur |  |  |
|  |  |
|  |  |
| Informatie en documentatie |  |  |
|  |  |
|  |  |
| Derden |  |  |
|  |  |
|  |  |

# Hoofdstuk III. Bijlagen

## 3.1. Bijlage 1 – Lijst van contacten

### 3.1.1 Intern

#### Disaster Response Team

| 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) |
| --- | --- | --- | --- |
| Disaster Recovery Manager |  |  |  |
| Back-up van de Manager |  |  |  |
| Disaster Recovery team |  |  |  |
| Back-up van de belangrijkste leden van het Disaster Recovery Team |  |  |  |
| .... |  |  |  |
| … |  |  |  |
|  |  |  |  |

#### Business Continuity Team

| **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 |

### 3.1.2 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 |
| ... |  |  |  |

## 3.2 Bijlage 2 - Nuttige documenten

* Business Continuity Plan
* Crisis Management Plan
* **[Technische specificaties]**
* …