**DISASTER RECOVERY PLAN TEMPLATE**

DISASTER RECOVERY PLAN

[ORGANISATIE]

[Locatie]
[Adres]

Versie [0.0.0]

Datum [00/00/0000]

| VERSIE GESCHIEDENIS |
| --- |
| VERSIE | GOEDGEKEURD DOOR | DATUM REVISIE | BESCHRIJVING VAN WIJZIGINGEN | AUTEUR |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **OPGESTELD DOOR** |  | **FUNCTIE** |  | **DATUM** |  |
| **GOEDGEKEURD DOOR** |  | **FUNCTIE** |  | **DATUM** |  |

**Disclaimer**

Dit document kan gebruikt worden als naslagwerk en sjabloon e voor het opzetten van een Disaster Recovery Plan (DRP) binnen jouw organisatie. De content van dit document bevat een aantal uitgangspunten die je zou kunnen opnemen in je eigen DRP. Niet alle uitgangspunten zullen van toepassing zijn, maak daarom een eigen afweging om bepaalde uitgangspunten wel of niet op te nemen. Naast de handreikingen in dit document is het belangrijk input te verzamelen van de verschillende afdelingen binnen de organisatie. Alle artikelen, sjablonen en informatie is uitsluitend bedoeld ter referentie. Hoewel wij ernaar streven de informatie actueel en correct te houden, geven wij geen enkele garantie, expliciet of impliciet, over de volledigheid, nauwkeurigheid, betrouwbaarheid, geschiktheid of beschikbaarheid van de website of de informatie, artikelen, sjablonen of gerelateerde afbeeldingen op de website.

# INHOUDSOPGAVE

[INHOUDSOPGAVE 3](#_Toc191384949)

[1. Hoofdlijnen Disaster Recovery Plan 4](#_Toc191384950)

[2. Rollen, verantwoordelijkheden, Contactgegevens 5](#_Toc191384951)

[3. Business Impact Analyse (BIA) 6](#_Toc191384952)

[4. Recovery Time Objective (RTO) 7](#_Toc191384953)

[5. Recovery Point Objective (RPO) 7](#_Toc191384954)

[6. Disaster Recovery Strategie 8](#_Toc191384955)

[7. Incident Respons 8](#_Toc191384956)

[8. Activatieplan 8](#_Toc191384957)

[a. Backup Procedures 9](#_Toc191384958)

[b. Disaster Recovery Procedures 9](#_Toc191384959)

[a. Cyber Recovery Procedures 9](#_Toc191384960)

[b. Recovery Plan voor Primaire Site 10](#_Toc191384961)

[c. Recovery Plan for uitwijklocatie 10](#_Toc191384962)

[d. Recovery Proces 10](#_Toc191384963)

[9. Testen en evalueren 11](#_Toc191384964)

[10. Plan Wijzigingen en Updates 11](#_Toc191384965)

# Hoofdlijnen Disaster Recovery Plan

Dit zijn de belangrijkste doelstellingen van het disaster recovery plan.

|  |
| --- |
| **Doelstellingen**Het is belangrijk om de scope en doelstellingen van het RDP helder te formuleren. Is het plan alleen van toepassing op de IT onderdelen van een organisatie of is het van toepassing op de gehele organisatie? Gaat het bijvoorbeeld alleen om de technologie in het datacenter of gaat het om de algehele technologie van een organisatie? Daarnaast is een bijbehorende planning onmisbaar. Een risicoanalyse kan helpen bij het bepalen van je scope. Tijdens een risicoanalyse ga je na wat de impact zou zijn op de business wanneer bepaalde bedrijf kritische applicaties of diensten niet meer geleverd kunnen worden. Om dit te kunnen doen, is het cruciaal om exact te weten welke applicaties en diensten op welke onderdelen van uw ICT-infrastructuur draaien en waar deze zich bevinden.[Beschrijf hier de doelstellingen]* SMART doelstelling 1
* SMART doelstelling 2
* SMART doelstelling 3

**Documentatie**Een DRP bevat naast bovenstaande informatie ook onderstaande elementen:• Contactgegevens van leveranciers,• Gekende herstelprocedures beschreven door deze leveranciers,• Systeem- en applicatie-inventarissen,• Netwerkbeschrijvingen en -schema’s,• Contracten en Service Level Agreements. |

# Rollen, verantwoordelijkheden, Contactgegevens

De belangrijkste resources betrokken bij het disaster recovery plan, inclusief alle belangrijke stakeholders en 3e partijen (zoals externe leveranciers).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **NAME & TITLE** | **ROL** | **TELEFOON** | **EMAIL** | **VERANTWOORDELIJK** |
| TTNL Support | Back-Up Leverancier | +31 (0)345 547040 | info@ttnl.nl | - |
| Nationaal Cyber Security Centrum | Meldpunt | +31 (0)70 751 55 55 | info@ncsc.nl  | - |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Business Impact Analyse (BIA)

Bij een Business Impact Analyse (BIA) wordt bekeken hoe de verschillende business units werken, welke bedrijfskritische processen afhankelijk zijn van IT en welke gevolgen bepaalde risico’s zouden kunnen hebben voor dat specifieke proces maar ook voor de andere bedrijfsactiviteiten.

De risico’s die je ziet, rangschik je op prioriteit. Hoe groot is de impact op het bedrijf als risico zich voltrekt? Zo zullen sommige risico’s impact hebben op de hele organisatie en andere slechts een klein onderdeel raken. Soms zullen de operationele en financiële verliezen groot zijn, soms is het minder gemakkelijk om de impact te kwantificeren, zoals bij reputatieschade.

Na zo’n BIA-analyse heb je een duidelijk beeld van alle mogelijke gevolgen van een incident voor een bedrijf, zowel de praktische problemen als de mogelijke kosten ervan. Het doel is om te bepalen hoe (in)tolerant de bedrijfskritische applicaties en -diensten zijn voor een mogelijke storing en wat de maximaal aanvaardbare downtime ervan mag zijn.

Daarna kun je de mogelijke opties evalueren om hun resistentie te verhogen en het risico op onderbreking te reduceren. Dit natuurlijk met de bedoeling om de dienstverlening binnen een aanvaardbare tijdsspanne te kunnen herstellen. Daarna volgt de RTO en RPO berekening.

|  |  |
| --- | --- |
|  | **IMPACT** |
| **FUNCTIE / PROCES** | RPO doelstelling | RTO Doelstelling | Maximale downtime | Prioriteit |
| LOGISTIEK | 24 uur | 24 uur | 72 uur | 1 |
| IT | 24 uur | 48 uur | 72 uur | 2 |
| FINANCE | 48 uur | 12 uur | 72 uur | 3 |
| SALES |  |  |  |  |
| HR |  |  |  |  |
| MARKETING |  |  |  |  |
| OPERATIONS |  |  |  |  |
| SERVICE DESK |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Recovery Time Objective (RTO)

Recovery Time Objective is de streeftijd waarbinnen een bepaalde functie, proces of dienst opnieuw operationeel moet zijn na een storing, om onaanvaardbare gevolgen voor de bedrijfsactiviteiten te vermijden.

Hierbij is het dus van belang om te berekenen hoe snel je organisatie zich moet kunnen herstellen, en op basis daarvan bepaal je welke maatregelen en budgetten nodig zijn om de bedrijfscontinuïteit zo goed mogelijk te verzekeren.

|  |
| --- |
|  |

# Recovery Point Objective (RPO)

Recovery Point Objective beschrijft het tijdsinterval dat mag voorbijgaan zonder dat de hoeveelheid verloren data de maximum toelaatbare drempel overschrijdt. De RPO wordt bepaald op basis van de tijd tussen 2 back-ups en de hoeveelheid gegevens die tussen die 2 back-ups verloren zouden kunnen gaan.

|  |
| --- |
|  |

# Disaster Recovery Strategie

Na de risicoanalyse, de BIA, het bepalen van de RTO en RPO en het in kaart brengen van het ICT landschap, kun je beginnen om concrete acties en procedures op te stellen waarop je kunt terugvallen wanneer een incident zich voordoet.

|  |
| --- |
|  |

# Incident Respons

Het DRP legt vast wie van het Disaster Recovery Team de ernst van de situatie in eerste instantie zal evalueren, het incident onder controle zal proberen krijgen en de nodige contactpersonen op de hoogte zal brengen.

|  |
| --- |
|  |

# Activatieplan

Aan de hand van de incidentevaluatie wordt besloten om het DRP (of onderdelen daarvan) te activeren. Het DRP beschrijft gedetailleerd en stap voor stap hoe gehandeld moet worden om het geraakte bedrijfsproces of netwerkelement zo snel en efficiënt mogelijk te herstellen of de taken ervan door een ander systeem te laten overnemen, zodat een normaal operationeel niveau bereikt kan worden.

|  |
| --- |
|  |

# Backup Procedures

Dit zijn de procedures die moeten worden uitgevoerd in geval van een ramp of een grote verstoring van processen.

|  |
| --- |
|  |

# Disaster Recovery Procedures

Dit zijn de belangrijkste onderdelen van het DRP die in noodgevallen onmiddellijk moeten worden aangepakt en waarop actie moet worden ondernomen.

|  |
| --- |
|  |

# Cyber Recovery Procedures

Dit zijn de belangrijkste onderdelen van het DRP die in het geval van cyber noodgevallen (hack, ransomware, rogue admin) onmiddellijk moeten worden aangepakt en waarop actie moet worden ondernomen.

|  |
| --- |
|  |

# Recovery Plan voor Primaire Site

Dit is de relevante informatie die nodig is om de herstelplannen op een mobiele locatie voort te zetten.

|  |
| --- |
| * Locatie datacenter
 |

# Recovery Plan for uitwijklocatie

Dit is de relevante informatie die nodig is om de herstelplannen en de normale bedrijfsvoering voort te zetten op een alternatieve of uitwijk-locatie.

|  |
| --- |
| * Locatie datacenter
* Contactgegevens leverancier
* SLA
 |

# Recovery Proces

Dit zijn de stappen en middelen die nodig zijn om de verstoorde systemen of bedrijfsvoering te herstellen.

|  |
| --- |
|  |

# Testen en evalueren

Evenals andere plannen is het belangrijk je DRP regelmatig te testen en te evalueren daar waar nodig. Dit kan bijvoorbeeld het geval zijn wanneer je vaststelt dat de gedefinieerde procedures niet de gewenste resultaten opleveren of de afgesproken RTO en RPO overschrijden.

Naast testen is het jaarlijks updaten van je DRP ook belangrijk. Een DRP met verouderde contact- en contractinformatie is schadelijjk omdat er kostbare tijd verloren zal gaan op cruciale momenten. Updaten is ook van belang wanneer je nieuwe activiteiten of diensten aan je organisatie toevoegt. Het loont dan om af te wegen welke impact deze nieuwe activiteiten en of diensten op je DRP hebben en in welke mate het DRP aangepast moet worden.

|  |
| --- |
|  |

# Plan Wijzigingen en Updates

Dit zijn de details over eventuele wijzigingen of updates in het DRP, het versienummer en de geschiedenis.

|  |
| --- |
|  |