Bedrijfscontinuïteit

***Over dit template:***

*Dit template is gemaakt door de mensen van ICT Institute.*

*Het template mag gratis worden gebruikt, onder een creative commons licentie*

[*https://creativecommons.org/licenses/by/4.0/*](https://creativecommons.org/licenses/by/4.0/)

*De nieuwste versie staat op:*

[*https://softwarezaken.nl/2022/01/gratis-27001-avg-templates/*](https://softwarezaken.nl/2022/01/gratis-27001-avg-templates/)

*Je mag het template uitbreiden, aanpassen en bewerken zoveel je wilt*

*Je mag het template en documenten gemaakt met het template doorgeven en delen zoveel je wilt*

*Als je het template doorgeeft, dan moet je "gemaakt door de mensen van ICT Institute" laten staan*

*Als je een document maakt met dit template en je bent geen opdrachtgever van ons, zet dat "gemaakt met template van ICT Institute" ergens in het document*

*Als je een opdrachtgever bent van ICT Institute, dan mag je alles doen met dit template wat je wilt*

*Let op dat je de ISO 27001 norm moet kopen bij NEN of een andere organisatie voordat je de norm gaat gebruiken. De norm is auteursrechtelijk beschermd*

*Lees vooral ook deze artikelen als je aan de slag gaat:*

[*https://softwarezaken.nl/2017/03/samenvatting-iso-27001-informatie-beveiliging/*](https://softwarezaken.nl/2017/03/samenvatting-iso-27001-informatie-beveiliging/)

[*https://softwarezaken.nl/2021/12/iso-27001-certificatie-aanvraag/*](https://softwarezaken.nl/2021/12/iso-27001-certificatie-aanvraag/)

[*https://softwarezaken.nl/2018/01/gdpr-avg-in-10-stappen/*](https://softwarezaken.nl/2018/01/gdpr-avg-in-10-stappen/)

[*https://softwarezaken.nl/security-verified/*](https://softwarezaken.nl/security-verified/)

# Achtergrond

## Over dit document

Dit document bevat de procedures voor Bedrijfscontinuïteit (BC) en Disaster Recovery (DR). Het behandelt ISO 27001:2022 maatregelen 5.29 en 5.30. Met dit document willen we een adequaat niveau van informatiebeveiliging behouden in het geval van gebeurtenissen die onze dagelijkse activiteiten verstoren en een solide plan opstellen om alles weer op de rails te krijgen. De veiligheid van het personeel is altijd het belangrijkste.

**Dit document moet op drie locaties worden bewaard:**

* Een digitale kopie in [GOOGLE DRIVE/SHAREPOINT/DROPBOX/ ENZ.]
* Een fysiek exemplaar in een afgesloten kast op kantoor
* Een fysiek exemplaar opgeslagen in een gesloten kast bij de CEO thuis

## Definities

**Maximum Tolerable Downtime (MTD):** Hoe lang een proces of systeem kan uitvallen voordat er onherstelbare schade wordt aangericht. *Voorbeeld: drie dagen voordat we klanten voorgoed verliezen.*

**Recovery Time Objective (RTO):** De maximale tijd die het mag duren voordat een proces of systeem weer operationeel is, altijd < MTD. *Voorbeeld: maximaal 24 uur.*

**Recovery Point Objective (RPO):** Het stadium/punt/versie dat een proces of systeem moet worden hersteld om weer als operationeel te worden beschouwd. *Voorbeeld: de meest recente dagelijkse back-up van de database.*

## Rollen en verantwoordelijkheden

Het BC-team bestaat uit:

|  |  |  |
| --- | --- | --- |
| **Rol en naam** | **Verantwoordelijkheden** | **Contactinformatie** |
| CEO, [NAAM] | Contact met autoriteiten, goedkeuring aankoop assets, beslissing over herplaatsing personeel | [NAAM@BEDRIJF.NL]  [TELEFOONNUMMER] |
| CISO [NAAM] | DR- en BC-coördinator, lessons learned | [NAAM@BEDRIJF.NL]  [TELEFOONNUMMER] |
| CTO, [NAAM] | Intern systeemherstel, softwareplatform herstel | [NAAM@BEDRIJF.NL]  [TELEFOONNUMMER] |
| COO, [NAAM] | Evacuatie personeel | [NAAM@BEDRIJF.NL]  [TELEFOONNUMMER] |
| Hoofd Juridisch, [NAAM] | Contact met verzekeringen, communicatie met stakeholders | [NAAM@BEDRIJF.NL]  [TELEFOONNUMMER] |

# Prioriteit van resources (Business Impact Analysis)

## Bedrijfscontinuïteitsdoelstellingen

[BEDRIJF] heeft de volgende vijf bedrijfscontinuïteitsdoelstellingen:

* Personeel veilig houden (hoofdprioriteit)
* Het standaard niveau van informatiebeveiliging handhaven
* Operationeel blijven om faillissement te voorkomen
* Terugkeren naar normale operatie binnen de beschreven RTO's
* Herstel systemen naar de beschreven RPO's

## Wettelijke- en contractuele eisen

We hebben de volgende wettelijke en contractuele verplichtingen met betrekking tot bedrijfscontinuïteit:

|  |  |
| --- | --- |
| **Bron** | **Eisen RTO en/of RPO** |
| Klanten die ons softwareplatform gebruiken | SLA van 99% op wekelijkse basis. RTO < 1u40. |
| … | [EISEN] |
| … | [EISEN] |

Naast de vereisten in de bovenstaande tabel, moet [BEDRIJF] mogelijk binnen 72 uur na een datalek een melding doen bij de Autoriteit Persoonsgegevens. [BEDRIJF] heeft hiervoor een datalekproces. [LINK PROCESDOCUMENT]

In de onderstaande tabel heeft [BEDRIJF] aangegeven wat het belang van elk proces is en welke systemen nodig zijn om ervoor te zorgen dat het proces operationeel is.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Proces** | **Assets nodig** | **MTD** | **RTO** | **RPO** |
| A. Sales | [CRM SYSTEEM, OFFICE SOFTWARE, EMAIL, MOBIELE TELEFOONS] | 1wk | 24u | 24u |
| B. Financiën | [VERWERKING BETALING (MOLLIE), FACTURATIE (MONEYBIRD)] | … | … | … |
| C. Online platform | [PRODUCTIEOMGEVING, PRODUCTIEDATABASE] | … | … | … |
| D. Service desk | [OFFICE SOFTWARE, KANTOORNETWERK / HUISNETWERK, SUPPORTSOFTWARE(ZENDESK)] | … | … | … |
| E. Software-ontwikkeling | [ACCEPTATIEOMGEVING, ONTWIKKELOMGEVING, KANTOORNETWERK / HUISNETWERK] | … | … | … |
| F. Marketing | [WEBSITE, MARKETINGSOFTWARE] | … | … | … |
| G. Operaties | [OFFICE SOFTWARE, KANTOORNETWERK] | … | … | … |

# Rampscenarios

## We hebben verschillende rampscenarios geïdentificeerd:

## Kantoor Amsterdam wordt onbruikbaar (brand, wateroverlast kantoor)

## Grote storing bij cloudleverancier – gevolgen voor de productieomgeving

## Crash productiedatabase

## Ransomware-aanval op pc's en laptops

## Ransomware-aanval op product

## Verlies van sleutelpersoneel (CEO, CTO)

## …

## Getroffen processen

Het effect van de rampscenario's op de processen van [BEDRIJF] is als volgt:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **A** | **B** | **C** | **D** | **E** | **F** | **G** | **.** |
| **1** | Y | N | . | . | . | . | . | . |
| **2** | N | Y | . | . | . | . | . | . |
| **3** | . | . | . | . | . | . | . | . |
| **4** | . | . | . | . | . | . | . | . |
| **5** | . | . | . | . | . | . | . | . |
| **6** | . | . | . | . | . | . | . | . |
| **.** | . | . | . | . | . | . | . | . |

## Respons

Reactie op een van de [AANTAL] rampscenario's heeft altijd twee processen: Disaster Recovery en Bedrijfscontinuïteit. Disaster Recovery is gericht op “*weer online komen*”. Bedrijfscontinuïteit is gericht op “*blijven bestaan*”. [BEDRIJF] zal bij de geconstateerde rampen als volgt handelen:

### Scenario 1: Kantoor Amsterdam wordt onbruikbaar

#### Disaster Recovery

Indien er personeel aanwezig is tijdens het evenement, worden zij direct geëvacueerd. Dit wordt geleid door het managementteam, dat tijdens de ontruiming 112 (brandweer/politie/ambulance) belt. Alle medewerkers komen indien mogelijk samen op [LOCATIE BUITEN].

#### Bedrijfscontinuïteit

Vragen om te beantwoorden:

* Verhuizen we naar een andere locatie OF werken we op afstand?
* Zoeken we een nieuwe kantoorruimte OF wachten we tot de oude veilig is verklaard?
* Wie neemt contact op met de IT-leverancier voor verloren hardware?

### Scenario 2: Grote storing bij cloudleverancier – productieomgeving uitgevallen

#### Disaster Recovery

…

#### Bedrijfscontinuïteit

…

### Scenario 3: Crash productiedatabase

#### Disaster Recovery

…

#### Bedrijfscontinuïteit

…

### Scenario 4: Ransomware-aanval op pc's en laptops

#### Disaster Recovery

…

#### Bedrijfscontinuïteit

…

### Scenario 5: Ransomware-aanval op product

#### Disaster Recovery

…

#### Bedrijfscontinuïteit

…

### Scenario 6: Verlies van sleutelpersoneel

#### Disaster Recovery

…

#### Bedrijfscontinuïteit

…

## Verificatie, review, en evaluatie

Bovenstaande maatregelen worden jaarlijks getoetst door middel van de volgende maatregelen:

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Scenario** | **Hoe te testen** | **Wanneer te testen** |
| 1 | Kantoor Amsterdam wordt onbruikbaar (brand, wateroverlast kantoor) | Iedereen werkt twee dagen thuis. [BRANDOEFENING?] | Jaarlijks, eerste week van maart |
| 2 | Grote storing bij cloudleverancier – productieomgeving uitgevallen | Productie klonen, offline halen om te zien of failover werkt. | Jaarlijks, derde week van maart |
| 3 | Crash productiedatabase | Back-up restore test. | n.v.t., zie nr. 4 |
| 4 | Ransomware-aanval op pc's en laptops | Wis en herstel één laptop op afstand volledig. | Jaarlijks, eerste week van maart |
| 5 | Ransomware-aanval op product | … | … |
| 6 | Verlies van sleutelpersoneel (CEO, CTO) | … | … |

Dit document wordt jaarlijks herzien om er zeker van te zijn dat alle relevante scenario's zijn opgenomen.