					Voer hier de naam van de geregistreerde rechtspersoon in						
Documentnummer: P32S					Documenttitel: **Beleid voor bedrijfscontinuïteit en disaster recovery**						
Versie: 1.0		Ingangsdatum: 01.01.2025			Documenteigenaar:						
X	Beleid		Standaard		Procedure		Formulier		Register		Overig

Revisiegeschiedenis				
Revisienummer	**Revisiedatum**	**Wijzigingen**	**Beoordeeld door**	**Proceseigenaar**

Goedkeuringen			
Naam	**Functie**	**Datum**	**Handtekening**

Afgestemd op normen en regelgeving

Norm/regelgeving	Clausule/artikel	Opmerking
ISO/IEC 27001:2022	Clausules 6.1, 6.3, 8	
ISO/IEC 27002:2022	Beheersmaatregelen 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-2, CP-4, CP-6, CP-7	
AVG	Artikelen 32, 33	
EU NIS2	Artikel 21(2)(f)	
EU DORA	Artikel 10	
COBIT 2019	DSS04	

1. Doel

1.1 Dit beleid waarborgt dat de organisatie de bedrijfsvoering kan voortzetten en essentiële IT-diensten kan herstellen tijdens en na verstorende gebeurtenissen, zoals stroomuitval, cyberaanvallen, ransomware-infecties of systeemstoringen.

1.2 Het biedt een duidelijk kader voor continuïteits- en herstelplanning, toegesneden op mkb-organisaties zonder eigen IT-afdeling.

1.3 Dit beleid ondersteunt de organisatie bij het voldoen aan toepasselijke vereisten uit hoofde van ISO/IEC 27001:2022, de AVG, NIS2, DORA en COBIT 2019, en draagt bij aan operationele weerbaarheid en klantvertrouwen.

2. Reikwijdte

2.1 Dit beleid is van toepassing op:

2.1.1 alle bedrijfskritische systemen en diensten (bijvoorbeeld e-mail, cloudopslag, factureringsplatforms en klantregistraties)

2.1.2 alle medewerkers en externe IT-dienstverleners die verantwoordelijk zijn voor de paraatheid en uitvoering van continuïteits- en herstelmaatregelen

2.1.3 alle typen verstoringen, waaronder cyberincidenten, hardwarestoringen, stroomuitval, overstromingen en ontoegankelijkheid van kantoorlocaties

2.2 Dit beleid omvat:

2.2.1 back-upbeheer

2.2.2 bedrijfscontinuïteitsplanning

2.2.3 herstelactiviteiten

2.2.4 opleiding van personeel en testen

2.2.5 juridische en regelgevende responsprocedures

3. Doelstellingen

3.1 Het vermogen van de organisatie beschermen om kernservices te leveren ondanks ongeplande verstoringen.

3.2 Tijdig herstel van systemen en gegevens waarborgen aan de hand van vooraf vastgestelde Recovery Time Objectives (RTO's).

3.3 Ervoor zorgen dat al het personeel tijdens crises de continuïteitsprocedures met minimale verwarring kan volgen.

3.4 Naleving waarborgen van wet- en regelgeving inzake gegevensbescherming en operationele weerbaarheid, waaronder artikel 32 van de AVG en artikel 21 van NIS2.

3.5 Een praktische, testbare continuïteits- en herstelstrategie vaststellen die geschikt is voor het mkb.

4. Rollen en verantwoordelijkheden

4.1 Algemeen directeur (GM)

4.1.1 is eigenaar van het continuïteits- en herstelproces en van dit beleid

4.1.2 keurt het bedrijfscontinuïteitsplan (BCP) goed

4.1.3 coördineert de incidentrespons en interne communicatie tijdens verstoringen

4.1.4 verzorgt meldingen aan toezichthouders indien vereist (bijvoorbeeld meldingen van datalekken onder de AVG)

4.2 IT-supportverlener / systeembeheerder

4.2.1 onderhoudt en test back-ups

4.2.2 voert herstelprocedures uit wanneer deze worden geactiveerd

4.2.3 documenteert alle herstelacties en gebeurtenissen rond systeemherstel

4.2.4 meldt kritieke IT-incidenten onmiddellijk aan de GM

[... Secties 4.3–8 zijn niet opgenomen in dit voorbeeld. Koop het volledige document voor toegang tot de volledige inhoud. ...]

9. Eisen voor herziening en bijwerking

9.1 Jaarlijkse herziening van beleid en plan

9.1.1 De algemeen directeur (GM) moet ervoor zorgen dat dit beleid en het bijbehorende bedrijfscontinuïteitsplan (BCP) ten minste eenmaal per jaar formeel worden beoordeeld.

9.1.2 De beoordeling moet ten minste het volgende omvatten:

9.1.2.1 evaluatie van nieuwe of opkomende risico's

9.1.2.2 hernieuwde validatie van RTO's/RPO's

9.1.2.3 verificatie van leveranciers- en contactinformatie

9.1.2.4 afstemming op wijzigingen in IT-systemen, wettelijke verplichtingen of bedrijfsvoering

9.2 Bijwerking op basis van triggers

9.2.1 Dit beleid moet ook worden bijgewerkt naar aanleiding van:

9.2.1.1 majeure incidenten of verstoringen, met name indien doelstellingen niet zijn gehaald

9.2.1.2 nieuwe wettelijke of regelgevende verplichtingen (bijvoorbeeld wijzigingen in DORA)

9.2.1.3 wijzigingen in kritieke systemen, cloudplatforms of personeel

9.2.1.4 bevindingen uit jaarlijkse BCP-/hersteltests

9.3 Proces voor wijzigingsbeheer

9.3.1 Alle wijzigingen moeten door de GM worden goedgekeurd

9.3.2 Er moet een versielogboek worden bijgehouden met daarin de datum, een beschrijving van de wijziging en de goedkeurder

9.3.3 Het bijgewerkte beleid moet opnieuw worden verspreid onder al het relevante personeel, waaronder de IT-supportverlener en afdelingshoofden

9.4 Documentatie van leerpunten

9.4.1 Gedocumenteerde leerpunten na tests of feitelijke verstoringen moeten worden verwerkt in toekomstige herzieningen

9.4.2 Deze beoordelingen moeten ook evaluaties van leverancierssprestaties en controles op de toereikendheid van de respons omvatten

10. Gerelateerde beleidslijnen en samenhang

10.1 Dit beleid is nauw geïntegreerd met de volgende mkb-beleidslijnen:

10.1.1 P1S – Informatiebeveiligingsbeleid: definieert de overkoepelende beveiligingsdoelstellingen die door continuïteits- en herstelpraktijken moeten worden ondersteund.

10.1.2 P4S – Beleid inzake toegangsbeheer: maakt noodintrekking of herstel van gebruikerstoegang mogelijk tijdens scenario's van bedrijfsverstoring.

10.1.3 P6S – Beleid inzake risicobeheer: vormt de basis voor het identificeren, evalueren en prioriteren van continuïteitsgerelateerde risico's.

10.1.4 P8S – Beleid inzake informatiebeveiligingsbewustzijn en opleiding: zorgt ervoor dat medewerkers voorbereid zijn om tijdens verstoringen te handelen en het BCP begrijpen.

10.1.5 P15S – Beleid inzake back-up en herstel: bevat specifieke technische procedures voor het waarborgen van de beschikbaarheid en het herstel van gegevens.

10.1.6 P17S – Beleid inzake gegevensbescherming en privacy: zorgt ervoor dat continuïteitsplanning de bescherming van persoonsgegevens respecteert en tijdens en na incidenten voldoet aan de AVG.

10.1.7 P22S – Beleid inzake logging en monitoring: ondersteunt de detectie van gebeurtenissen die continuïteits- en herstelprocessen kunnen activeren en levert forensische audittrails na verstoringen.

10.1.8 P30S – Incidentresponsbeleid (P30): gaat direct vooraf aan de activering van het herstelproces bij cyber- of operationele incidenten.

10.1.9 P31S – Beleid inzake bewijsverzameling en forensisch onderzoek: zorgt ervoor dat digitaal bewijsmateriaal tijdens continuïteitsscenario's wordt vastgelegd voor nalevings-, verzekerings- of onderzoeksdoeleinden.

10.2 Deze beleidslijnen vormen samen een samenhangend, auditgereed kader voor weerbaarheid, verantwoording en continuïteit van beheersmaatregelen binnen alle mkb-activiteiten.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001:

11.1.1 Clausule 6.1 – Vereist risicogebaseerde planning en behandeling, waaronder bedrijfscontinuïteit en herstel.

11.1.2 Clausule 6.3 – Benadrukt continue verbetering na verstoringen.

11.1.3 Clausule 8.1 – Verplicht operationele beheersmaatregelen, waaronder gedocumenteerde continuïteitsmaatregelen.

11.2 ISO/IEC 27002:

11.2.1 Beheersmaatregel 5.29 – Vereist het opzetten en onderhouden van regelingen voor bedrijfscontinuïteit.

11.2.2 Beheersmaatregel 5.30 – Vereist het testen en beoordelen van deze regelingen.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-2 – Definieert vereisten voor continuïteitsplanning.

11.3.2 CP-4 – Verplicht continuïteitstraining voor personeel van de organisatie.

11.3.3 CP-6 – Omvat vereisten voor alternatieve opslaglocaties.

11.3.4 CP-7 – Stelt eisen aan alternatieve verwerkingslocaties.

11.4 AVG:

11.4.1 Artikel 32 – Vereist maatregelen om de voortdurende beschikbaarheid en weerbaarheid van verwerkingssystemen en -diensten te waarborgen.

11.4.2 Artikel 33 – Activeert meldingsverplichtingen bij inbreuken wanneer een continuïteitsfalen leidt tot compromittering van persoonsgegevens.

11.5 EU NIS2-richtlijn (2022/2555):

11.5.1 Artikel 21(2)(f) – Vereist continuïteitsplanning en crisisbeheercapaciteiten als voorwaarde voor gereedheid ten aanzien van cyberrisico's.

11.6 EU DORA-verordening (2022/2554):

11.6.1 Artikel 10 – Verplicht de implementatie van testen voor digitale operationele weerbaarheid en herstelcapaciteiten, met name voor mkb-organisaties in de financiële sector.

11.7 COBIT 2019:

11.7.1 DSS04 – Continuïteit beheren: biedt richtlijnen voor enterprise governance voor het handhaven en valideren van operationele weerbaarheid, waaronder eigenaarschap, testen, integratie van leveranciers en beoordelingen na gebeurtenissen.