					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P32					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	Clausule 8	
ISO/IEC 27002:2022	Beheersmaatregelen 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-1 t/m CP-11	
NIST SP 800-34 Rev.1	Continuïteitsplanning	Raamwerk
ISO 22301:2019		Vereisten voor managementsystemen voor bedrijfscontinuïteit
EU AVG	Artikel 32	
EU NIS2	Artikel 21(2)(f)	
EU DORA	Artikel 10	
COBIT 2019	DSS	

1. Doel

1.1. Dit beleid stelt verplichte beheersmaatregelen en verantwoordelijkheden vast om te waarborgen dat de organisatie kritieke bedrijfsactiviteiten en ondersteunende ICT-diensten tijdens en na een verstorend incident kan voortzetten of herstellen.

1.2. Dit beleid heeft tot doel levens, operationele stabiliteit, wettelijke verplichtingen, klantverplichtingen en de reputatie van de organisatie te beschermen door weerbaarheid te verankeren via proactieve planning en gevalideerde herstelcapaciteiten.

1.3. Dit beleid vormt de basis voor het raamwerk van de organisatie voor bedrijfscontinuïteitsbeheer (BCM) en disaster recovery (DR) en waarborgt naleving van toepasselijke wettelijke, contractuele en branchevereisten.

2. Reikwijdte

2.1. Dit beleid is van toepassing op alle organisatieonderdelen, informatiesystemen, bedrijfsprocessen, medewerkers en diensten van derden die op basis van de resultaten van de Business Impact Analysis (BIA) als kritisch of essentieel zijn geclassificeerd.

2.2. Dit beleid omvat:

2.2.1. Natuurlijke en door mensen veroorzaakte verstoringen, waaronder cyberaanvallen, uitval van infrastructuur, uitval van datacenters, pandemieën en onderbrekingen in leveranciersdiensten

2.2.2. Planning, testen en continue verbetering van bedrijfscontinuïteitsplannen (BCP's) en disaster recovery-plannen (DRP's)

2.2.3. Rollen en verantwoordelijkheden voor noodrespons, herstelcoördinatie en incidentescalatie

2.3. Alle medewerkers met verantwoordelijkheden op het gebied van continuïteit of herstel, waaronder IT, proceseigenaren, crisisteammedewerkers en leveranciers, vallen onder de bepalingen van dit beleid.

3. Doelstellingen

3.1. Het waarborgen van de continuïteit van bedrijfsactiviteiten en diensten door middel van vooraf gedefinieerde en geteste procedures, met minimale operationele, reputatie- en juridische impact.

3.2. Het herstellen van ICT-diensten binnen vastgestelde hersteltijddoelstellingen (RTO's) en herstelpuntdoelstellingen (RPO's), afgestemd op de risicotolerantie van de organisatie.

3.3. Het toewijzen van eigenaarschap voor de planning, uitvoering en governance van bedrijfscontinuïteit en disaster recovery binnen de gehele organisatie.

3.4. Het waarborgen dat continuïteitscapaciteiten regelmatig worden getest, onderhouden en verbeterd op basis van realistische scenario's en auditbevindingen.

3.5. Het voldoen aan nalevingsverplichtingen op grond van ISO, NIST, AVG, DORA en NIS2 ter ondersteuning van zorgvuldigheid op het gebied van operationele weerbaarheid en beschikbaarheid.

4. Rollen en verantwoordelijkheden

4.1. Directie

4.1.1. Keurt het beleid voor bedrijfscontinuïteit en disaster recovery goed en waarborgt de strategische afstemming.

4.1.2. Wijst budget en middelen toe ter ondersteuning van bedrijfscontinuïteit, noodrespons en hersteloefeningen.

4.2. Manager bedrijfscontinuïteit (BCM-lead)

4.2.1. Is eigenaar van de ontwikkeling en het onderhoud van organisatiebrede BCP's en van de coördinatie van continuïteitstests.

4.2.2. Beheert de BIA-planning, faciliteert training en waarborgt dat de documentatie voldoet aan nalevingseisen.

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

9. Vereisten voor beoordeling en actualisering

9.1. Dit beleid moet jaarlijks worden beoordeeld door de manager bedrijfscontinuïteit en de CISO om afstemming te waarborgen met:

9.1.1. Wijzigingen in bedrijfsactiviteiten, kritieke systemen of infrastructuur

9.1.2. Lessen uit incidenten, audits, tabletop-oefeningen of DR-tests

9.1.3. Geactualiseerde wettelijke of contractuele verplichtingen (bijvoorbeeld DORA, AVG, RTO/RPO-vereisten van klanten)

9.1.4. Wijzigingen in de risicobereidheid of continuïteitsstrategie van de organisatie

9.2. Beoordelingen moeten het volgende omvatten:

9.2.1. Validatie van de relevantie van plannen en contactgegevens

9.2.2. Herbeoordeling van RTO's, RPO's en herstelclassificatie in niveaus

9.2.3. Evaluatie van de capaciteit van back-up- en DR-diensten

9.2.4. Feedback van belanghebbenden die recente herstelplannen of tests hebben uitgevoerd

9.3. Alle beleidswijzigingen moeten:

9.3.1. Onder versiebeheer staan met gedocumenteerde onderbouwing en goedkeuring door belanghebbenden

9.3.2. Worden gecommuniceerd aan sleutelmedewerkers en teams met geactualiseerde verantwoordelijkheden

9.3.3. Worden verwerkt in geactualiseerde training, bewustwordingsmaterialen en operationele procedures

9.4. Tijdelijke spoedactualisaties moeten worden uitgegeven indien sprake is van een grote organisatorische wijziging, een wettelijke verplichting of een kritieke bevinding waardoor de huidige plannen of het beleid niet langer uitvoerbaar zijn.

10. Gerelateerde beleidsdocumenten en samenhang

10.1. Dit beleid hangt samen met de volgende kerndocumenten:

10.1.1. P1 – Informatiebeveiligingsbeleid: Stelt de eis vast voor risicogebaseerde, weerbare bedrijfsvoering onder alle omstandigheden.

10.1.2. P5 – Wijzigingsbeheerbeleid: Waarborgt dat configuratie- of infrastructuurwijzigingen die verband houden met herstel gedocumenteerde en goedgekeurde workflows volgen.

10.1.3. P14 – Beleid voor bewaartermijnen en verwijdering van gegevens: Regelt de levenscyclus van back-upmedia en herstelde gegevens die worden gebruikt bij continuïteitsactiviteiten.

10.1.4. P15 – Back-up- en herstelbeleid: Verplicht beheersmaatregelen voor back-upfrequentie, beveiliging en verificatie van herstel.

10.1.5. P18 – Beleid voor cryptografische beheersmaatregelen: Waarborgt dat herstelprocessen voldoen aan normen voor versleuteling en vertrouwelijkheid.

10.1.6. P22 – Beleid voor logging en monitoring: Ondersteunt de detectie en escalatie van gebeurtenissen die impact hebben op continuïteit.

10.1.7. P30 – Incidentresponsbeleid: Definieert processen voor beheersing, escalatie en oorzaakanalyse die zijn afgestemd op continuïteitstriggers.

10.1.8. P33 – Beleid voor audit en nalevingstoezicht: Valideert de integriteit en effectiviteit van continuïteits- en herstelpraktijken binnen systemen en processen.

11. Referentienormen en raamwerken

11.1. Dit beleid is afgestemd op internationaal erkende normen voor bedrijfscontinuïteit en disaster recovery en ondersteunt auditbaarheid, weerbaarheid en wettelijke naleving.

11.2. ISO/IEC 27002

11.2.1. Bijlage A beheersmaatregel 5.29 – Informatiebeveiliging tijdens verstoringen: Vereist continuïteit van beveiligingsmaatregelen onder ongunstige omstandigheden.

11.2.2. Bijlage A beheersmaatregel 5.30 – ICT-gereedheid voor bedrijfscontinuïteit: Verplicht de voorbereiding, het testen en de validatie van ICT-herstelcapaciteiten.

11.3. ISO 22301:2019 – Managementsystemen voor bedrijfscontinuïteit

11.3.1. Biedt het raamwerk voor het vaststellen, implementeren en onderhouden van BCM-praktijken die zijn afgestemd op organisatiedoelstellingen en risicodrempels.

11.4. NIST SP 800-34 Rev.1 – Richtlijn voor continuïteitsplanning

11.4.1. Beschrijft best practices voor continuïteitsplannen voor IT-systemen, waaronder de ontwikkeling van continuïteitsstrategieën, impactanalyse en het testen van plannen.

11.5. EU AVG (2016/679)

11.5.1. Artikel 32 – Beveiliging van de verwerking: Vereist weerbaarheid van verwerkingssystemen en tijdig herstel van de beschikbaarheid van en toegang tot persoonsgegevens na een incident.

11.6. EU NIS2-richtlijn (2022/2555)

11.6.1. Artikel 21(2)(f): Verplicht maatregelen voor bedrijfscontinuïteit en crisisbeheer ter ondersteuning van de beveiliging van netwerk- en informatiesystemen.

11.7. EU DORA (2022/2554)

11.7.1. Artikel 10 – ICT-bedrijfscontinuïteit: Vereist dat financiële entiteiten ICT-continuïteitsplannen ontwikkelen en testen, inclusief risicogebaseerde RTO/RPO's en failovercapaciteiten.

11.8. COBIT 2019

11.8.1. DSS04 – Continuïteit beheren: Omvat alle aspecten van continuïteitsplanning, waaronder dreigingsidentificatie, impactanalyse, herstelstrategie en periodiek testen.