					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P15S					Documenttitel: **Back-up- en herstelbeleid**							
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	Beheersmaatregelen voor back-up in overeenstemming met de vereisten van het ISMS
ISO/IEC 27002:2022	Beheersmaatregelen 5.29, 8	Best practices voor back-up en integratie met het bedrijfscontinuïteitsplan
NIST SP 800-53 Rev.5	CP-9, MP-6	Back-up en bescherming van media
EU NIS2	Artikel 21(2)(c)	Weerbaarheid en continuïteit door middel van back-up
EU DORA	Artikel 10(1)	ICT-continuïteit – back-up voor financiële organisaties
COBIT 2019	BAI04.05, DSS04	Back-ups documenteren en testen, beheersprocessen inrichten
AVG	Artikelen 5(1)(f), 32(1)(c)	Integriteit, beschikbaarheid en tijdig herstel van gegevens

1. Doel

1.1 Dit beleid bepaalt hoe de organisatie back-ups uitvoert en beheert om de bedrijfscontinuïteit te waarborgen, gegevensverlies te voorkomen en tijdig herstel na incidenten mogelijk te maken.

1.2 Het stelt bindende regels vast voor de wijze waarop systemen en gegevens moeten worden geback-upt, opgeslagen en hersteld, in het bijzonder binnen mkb-organisaties zonder complexe IT-infrastructuur.

1.3 Dit beleid ondersteunt auditgereedheid en ISO/IEC 27001-certificering door te waarborgen dat essentiële back-upbeheersmaatregelen aanwezig zijn, consistent worden toegepast en periodiek worden beoordeeld.

1.4 Het vermogen van de organisatie om te herstellen van technische storingen, onbedoelde verwijdering of cyberincidenten is afhankelijk van strikte naleving van dit beleid.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle bedrijfssystemen en gegevens, waaronder:

2.1.1 financiële administraties, klantinformatie en HR-gegevens

2.1.2 desktops, laptops, servers en cloudtoepassingen die worden gebruikt in de bedrijfsvoering

2.1.3 back-upmedia, zoals USB-drives, externe opslagmedia of cloudgebaseerde back-ups

2.2 Dit beleid is tevens van toepassing op alle personen die verantwoordelijk zijn voor de uitvoering of het beheer van back-upprocessen, waaronder:

2.2.1 de algemeen directeur (GM) of een aangewezen verantwoordelijke

2.2.2 externe IT-dienstverleners of adviseurs

2.2.3 alle medewerkers die verantwoordelijk zijn voor het opslaan van gegevens op goedgekeurde locaties

3. Doelstellingen

3.1 Waarborgen dat alle kritieke bedrijfsgegevens en systemen veilig worden geback-upt met passende intervallen op basis van risico en operationele noodzaak.

3.2 Waarborgen dat gegevens na verstoringen tijdig en volledig kunnen worden hersteld.

3.3 Voorkomen van ongeautoriseerde toegang tot, manipulatie van of verlies van back-upgegevens door middel van doeltreffende opslagbeheersmaatregelen.

3.4 Rollen en verantwoordelijkheden voor de implementatie en toetsing van back-upprocedures duidelijk toewijzen en handhaven.

3.5 Naleving van ISO/IEC 27001, de AVG en andere wettelijke en reglementaire verplichtingen ondersteunen door middel van gestructureerde en gedocumenteerde back-uppraktijken.

4. Rollen en verantwoordelijkheden

4.1 Algemeen directeur (GM)

4.1.1 keurt dit beleid goed en ziet toe op de naleving ervan

4.1.2 wijst middelen toe en belegt de verantwoordelijkheid voor back-up- en herstelactiviteiten

4.1.3 beoordeelt back-upfouten, incidenten of beleidsafwijkingen

4.1.4 leidt de jaarlijkse beleidsbeoordeling en waarborgt auditgereedheid

4.2 Externe IT-dienstverlener (indien van toepassing)

4.2.1 implementeert en beheert back-upoplossingen (lokaal of cloudgebaseerd)

4.2.2 bewaakt het slagen van back-ups en plant hersteltests

4.2.3 meldt fouten en incidenten rechtstreeks aan de GM

4.2.4 waarborgt versleuteling, toegangsbeperkingen en correcte omgang met back-upmedia

[... 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 actualisatie

9.1 Dit beleid moet ten minste eenmaal per jaar door de GM worden beoordeeld. Aanleidingen voor tussentijdse beoordelingen zijn onder meer:

9.1.1 majeure wijzigingen in systemen of opslagmethoden

9.1.2 invoering van nieuwe cloud- of IT-platforms

9.1.3 juridische of reglementaire wijzigingen die gevolgen hebben voor gegevensherstel

9.1.4 bevindingen uit audits of incidenten

9.2 De GM is verantwoordelijk voor het initiëren van de beoordeling, het goedkeuren van wijzigingen en het communiceren van actualisaties.

9.3 Beleidsversies moeten worden bijgehouden en gearchiveerd. Vervangen versies moeten in toegang worden beperkt om verwarring tijdens audits of herstel na verstoringen te voorkomen.

10. Gerelateerde beleidsdocumenten en samenhang

10.1 Dit beleid is afgestemd op en afhankelijk van de volgende mkb-beleidsdocumenten:

10.1.1 P14S – Gegevensbewaringsbeleid en verwijderingsregels: bepaalt hoe lang back-upgegevens moeten worden bewaard en veilig verwijderd.

10.1.2 P13S – Beleid inzake gegevensclassificatie en etikettering: ondersteunt de prioritering van gegevens die op basis van classificatieniveaus moeten worden geback-upt.

10.1.3 P30S – Incidentresponsbeleid: beschrijft de procedures wanneer back-ups mislukken of wanneer gegevensherstel nodig is na een inbreuk of uitval.

10.1.4 P2S – Beleid inzake governancerollen en -verantwoordelijkheden: wijst duidelijke bevoegdheden toe voor toezicht op back-ups en handhaving van beleid.

10.1.5 P17S – Beleid inzake gegevensbescherming en privacy: waarborgt dat de omgang met persoonsgegevens in back-ups in lijn is met wet- en regelgeving en privacyvereisten.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001

11.1.1 Clausule 8.1: operationele planning en beheersing van back-upsystemen als onderdeel van het ISMS

11.2 ISO/IEC 27002

11.2.1 Beheersmaatregel 8.13: beschrijft best practices voor planning, monitoring en herstel van back-ups

11.2.2 Bijlage A, beheersmaatregel 5.29: integratie van back-up met bedrijfscontinuïteit en herstelgereedheid

11.3 NIST SP 800-53 Rev.5

11.3.1 CP-9 (Contingency Planning): definieert gestructureerde back-upstrategieën voor bedrijfsweerbaarheid

11.3.2 MP-6 (Media Protection): vereist veilige omgang met en vernietiging van back-upmedia

11.4 AVG

11.4.1 Artikel 5(1)(f): vereist integriteit en beschikbaarheid van persoonsgegevens

11.4.2 Artikel 32(1)(c): vereist het vermogen om de toegang tot persoonsgegevens tijdig te herstellen

11.5 EU NIS2-richtlijn

11.5.1 Artikel 21(2)(c): vereist back-up en herstel als onderdeel van weerbaarheids- en continuïteitsplanning

11.6 EU DORA

11.6.1 Artikel 10(1): organisaties in de financiële sector moeten back-up waarborgen als onderdeel van ICT-continuïteitsmaatregelen

11.7 COBIT 2019

11.7.1 BAI04.05: vereist gedocumenteerde back-upstrategieën

11.7.2 DSS04.07: benadrukt routinematige toetsing en beheersing van back-up- en gegevensherstelprocessen