					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P27S					Documenttitel: **Beleid inzake het gebruik van cloudservices**							
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 5.23–5.25	
NIST SP 800-53 Rev. 5	AC-20, SC-12, SC-13, SR-5	
AVG	Artikel 28, 32 en hoofdstuk V	
EU NIS2	Artikelen 21(2)(f), (i)	
EU DORA	Artikelen 5(2), 28	
COBIT 2019	DSS01, DSS05, BAI04	

1. Doel

1.1 Dit beleid bepaalt hoe de organisatie op veilige wijze gebruikmaakt van in de cloud gehoste diensten. Het waarborgt dat gegevens die in de cloud worden verwerkt of opgeslagen, adequaat worden beschermd, dat toegang wordt beheerst en dat risico's op verantwoorde wijze worden beheerd.

1.2 Dit beleid helpt mkb-organisaties te voldoen aan wettelijke verplichtingen en klantverwachtingen ten aanzien van de bescherming van gevoelige informatie, het voorkomen van datalekken en het doeltreffend beheersen van cloudgerelateerde risico's, zonder dat infrastructuur op enterprise-niveau vereist is.

1.3 Dit beleid ondersteunt ISO/IEC 27001-certificering, naleving van de AVG en assurance binnen de toeleveringsketen door consistente governance van alle clouddiensten van derden.

2. Reikwijdte

2.1 Dit beleid is van toepassing op:

2.1.1 alle cloudgebaseerde diensten die worden gebruikt voor het opslaan, verwerken of verzenden van bedrijfsgegevens

2.1.2 alle medewerkers, contractanten en dienstverleners die namens de organisatie cloudtools gebruiken

2.1.3 gratis en betaalde cloudoplossingen, waaronder e-mailplatforms, documentdeling, SaaS-tools, back-upplatforms, videoconferencing en klantplatforms

2.1.4 elk apparaat (desktop, mobiel apparaat, tablet) dat via cloudtoepassingen toegang heeft tot bedrijfsinformatie

2.2 Dit omvat onder meer:

2.2.1 Microsoft 365, Google Workspace, Dropbox Business

2.2.2 Zoom, Microsoft Teams, Google Meet

2.2.3 AWS, Azure, GCP

2.2.4 cloudgebaseerde tools voor back-up en disaster recovery

2.2.5 gedeelde mappen of applicaties die worden gebruikt voor facturatie, projectbeheer of klantcommunicatie

3. Doelstellingen

3.1 Voorkomen van ongeautoriseerd of risicovol gebruik van niet-goedgekeurde clouddiensten.

3.2 Waarborgen dat gevoelige of gereguleerde gegevens die in de cloud zijn opgeslagen, worden beveiligd met passende technische en organisatorische beheersmaatregelen.

3.3 Duidelijke rollen vaststellen voor het goedkeuren, configureren, monitoren en uitfaseren van clouddiensten.

3.4 Gegevensstromen beheersen en verplichtingen inzake bewaartermijnen, verwijdering en privacy afdwingen voor in de cloud opgeslagen informatie.

3.5 De afhankelijkheid van persoonlijke accounts of niet-beheerde tools verminderen door goedkeuring te vereisen voor alle cloudsystemen die voor zakelijke doeleinden worden gebruikt.

3.6 Voldoen aan de vereisten van ISO/IEC 27001:2022, de AVG, NIS2 en DORA voor het beheersen van afhankelijkheden van externe cloudleveranciers.

4. Rollen en verantwoordelijkheden

4.1 Algemeen directeur

4.1.1 keurt het gebruik van alle nieuwe clouddiensten goed

4.1.2 beoordeelt risico's met betrekking tot cloudleveranciers en typen dienstverlening

4.1.3 handhaaft dit beleid en houdt toezicht op besluiten over uitzonderingen

4.2 IT-dienstverlener of technische ondersteuning

4.2.1 beoordeelt en implementeert veilige configuraties voor clouddiensten

4.2.2 richt accounts, toegangsbeheersmaatregelen en back-ups in

4.2.3 monitort de naleving van wachtwoord-, multifactorauthenticatie- en beveiligingsinstellingen

[... 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 actualisering

9.1 Dit beleid moet ten minste jaarlijks worden beoordeeld door de algemeen directeur, in afstemming met de IT-dienstverlener.

9.2 Een formele beoordeling moet ook plaatsvinden:

9.2.1 na een cloudgerelateerd beveiligingsincident, zoals een inbreuk of gegevensverlies

9.2.2 wanneer een nieuw groot cloudplatform wordt ingevoerd

9.2.3 wanneer wettelijke of regelgevende vereisten wijzigen, zoals updates van de AVG, NIS2 of DORA

9.2.4 als monitoringactiviteiten misbruik of nieuwe risico's aan het licht brengen

9.3 De algemeen directeur moet waarborgen dat:

9.3.1 het register van clouddiensten wordt bijgewerkt met nieuwe of uitgefaseerde diensten

9.3.2 blijvend wordt voldaan aan wettelijke en privacyvereisten

9.3.3 alle wijzigingen worden gecommuniceerd aan relevante gebruikers en belanghebbenden

9.4 Gearchiveerde versies moeten veilig worden opgeslagen en oude beleidsversies moeten worden beheerd in overeenstemming met het P14S – Gegevensbewarings- en vernietigingsbeleid van de organisatie.

10. Gerelateerde beleidslijnen en samenhang

10.1 Dit beleid moet worden toegepast in samenhang met de volgende op het mkb afgestemde beleidslijnen inzake informatiebeveiliging:

10.1.1 P2S – Beleid inzake governancerollen en -verantwoordelijkheden: definieert de verantwoordingsplicht voor het goedkeuren van clouddiensten en het beheren van relaties met dienstverleners.

10.1.2 P4S – Beleid inzake toegangscontrole: ondersteunt veilige aanmelding, sessiebeheer en procedures voor intrekking van toegangsrechten die voor cloudplatforms vereist zijn.

10.1.3 P14S – Gegevensbewarings- en vernietigingsbeleid: regelt hoe cloudgebaseerde gegevens worden geback-upt, bewaard en verwijderd in overeenstemming met wettelijke verplichtingen.

10.1.4 P17S – Beleid inzake gegevensbescherming en privacy: waarborgt dat persoonsgegevens die in clouddiensten zijn opgeslagen, worden verwerkt volgens de beginselen van de AVG.

10.1.5 P30S – Incidentresponsbeleid (P30): biedt gestructureerde procedures voor respons op cloudbeveiligingsincidenten, inclusief bewijsverzameling en externe melding.

10.2 Deze beleidslijnen waarborgen gezamenlijk dat cloudgebruik veilig, compliant en operationeel weerbaar is.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001

11.1.1 Clausule 8.1 – vereist dat organisaties operationele beheersmaatregelen implementeren voor gegevensverwerking, met inbegrip van beheersmaatregelen voor cloudgebaseerde systemen.

11.2 ISO/IEC 27002

11.2.1 Beheersmaatregel 5.23 – vereist governance over het gebruik van clouddiensten en SaaS-tools van derden.

11.2.2 Beheersmaatregel 5.24 – vereist een vastgesteld cloudbeleid dat is afgestemd op risico's en regelgevende vereisten.

11.2.3 Beheersmaatregel 5.25 – vereist dat organisaties waarborgen dat beveiligingsmaatregelen in cloudomgevingen aansluiten op de behoeften van de organisatie.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AC-20 – vereist formeel gebruiksbeleid voor externe systemen zoals clouddiensten.

11.3.2 SC-12, SC-13 – behandelen encryptie voor gegevens tijdens transport en gegevens in rust binnen cloudomgevingen.

11.3.3 SR-5 – omvat beheersmaatregelen voor cloud- en derdenrisico's binnen de toeleveringsketen.

11.4 AVG (Verordening (EU) 2016/679)

11.4.1 Artikel 28 – vereist dat cloudproviders die optreden als verwerker bindende contractuele verplichtingen naleven.

11.4.2 Artikel 32 – schrijft technische en organisatorische maatregelen voor cloudgebaseerde gegevensverwerking voor.

11.4.3 Hoofdstuk V – verbiedt niet-geautoriseerde internationale doorgiften van persoonsgegevens die in de cloud zijn opgeslagen.

11.5 EU NIS2-richtlijn (2022/2555)

11.5.1 Artikel 21(2)(f), (i) – vereist dat essentiële en belangrijke entiteiten passende beleidslijnen implementeren voor de beveiliging van clouddiensten en de beheersing van de toeleveringsketen.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 5(2) – vereist dat financiële mkb-organisaties cloudbeveiliging integreren in hun ICT-risicobeheerkaders.

11.6.2 Artikel 28 – stelt toezichtregels vast voor kritieke externe ICT-dienstverleners, waaronder cloudleveranciers.

11.7 COBIT 2019

11.7.1 DSS01 – "Manage Operations" behandelt de operationele integriteit van clouddiensten.

11.7.2 DSS05 – "Manage Security Services" omvat cloudspecifieke beschermingsmaatregelen en monitoring.

11.7.3 BAI04 – "Manage Availability and Capacity" waarborgt bedrijfscontinuïteit en prestaties in cloudomgevingen.