					Voer hier de naam van de geregistreerde rechtspersoon in						
Documentnummer: P26S					Documenttitel: **Beleid inzake beveiliging van derde partijen en leveranciers**						
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	Operationele beheersmaatregelen voor relaties met derde partijen en leveranciers
ISO/IEC 27002:2022	Beheersmaatregelen 5.19–5.22	Beheersmaatregelen voor leveranciersbeveiliging, contractuele beveiligingsvoorwaarden, wijzigingsbeheer, monitoring en beoordeling
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Verwerving, configuratie, interconnectieovereenkomsten en beheersmaatregelen voor extern personeel
AVG	Artikelen 28, 32	Verwerkersovereenkomsten, beveiligingsvereisten voor verwerkers
EU NIS2	Artikelen 21(2)(a)(b)(i), 23(1)	Risicobeheer in de toeleveringsketen, toezicht op diensten van derden
EU DORA	Artikelen 5(1)(2), 28(1)(2)	ICT-risicobeheer voor ICT-dienstverleners van derde partijen
COBIT 2019	APO10, APO12, DSS05	Leveranciersmanagement en integratie van risico's

1. Doel

1.1 Dit beleid stelt de verplichte beveiligingsvereisten vast voor het aangaan, beheren en beëindigen van relaties met derde partijen en leveranciers die toegang hebben tot of invloed uitoefenen op de gegevens, systemen of diensten van de organisatie.

1.2 Het waarborgt dat externe dienstverleners — waaronder IT-supportverleners, cloudproviders, softwareontwikkelaars en opdrachtnemers voor bedrijfsprocessen — bedrijfsmiddelen veilig behandelen, in overeenstemming met toepasselijke wet- en regelgeving en normen.

1.3 Dit beleid beperkt risico's zoals datalekken, ongeautoriseerde systeemwijzigingen, boetes van toezichthouders of verstoringen van de bedrijfsvoering als gevolg van onveilige of onvoldoende beheerde afspraken met derde partijen.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle derde partijen die:

2.1.1 software, infrastructuur, hosting of clouddiensten leveren

2.1.2 toegang hebben tot of beheer uitvoeren op interne systemen, apparaten of applicaties

2.1.3 bedrijfsgegevens, documenten of back-ups verwerken

2.1.4 bedrijfsactiviteiten, HR, financiën of klantdiensten ondersteunen

2.2 Dit beleid is ook van toepassing op:

2.2.1 interne medewerkers die betrokken zijn bij het selecteren, contracteren of aansturen van leveranciers

2.2.2 alle medewerkers die leveranciersonboarding, contracten, toegang of beoordelingen beheren

2.2.3 elk systeem of proces dat afhankelijk is van componenten of diensten van derde partijen

3. Doelstellingen

3.1 Waarborgen dat alle leveranciers voldoen aan duidelijk vastgestelde beveiligingseisen.

3.2 Vereisen dat leverancierscontracten afdwingbare verplichtingen bevatten inzake beveiliging, privacy en incidentrespons.

3.3 Leveranciersrisico's beoordelen en documenteren voordat overeenkomsten worden ondertekend of toegang wordt verleend.

3.4 Periodieke beoordelingen uitvoeren bij kritieke leveranciers of leveranciers met een hoog risico om naleving te bevestigen.

3.5 Een formeel proces vaststellen voor uitzonderingen, incidentbeheer en contractactualisaties.

3.6 Ondersteunen van naleving van verplichtingen uit hoofde van ISO/IEC 27001:2022, de AVG, NIS2 en DORA met betrekking tot leveranciersgovernance.

4. Rollen en verantwoordelijkheden

4.1 Algemeen directeur (GM)

4.1.1 Draagt de eindverantwoordelijkheid voor leveranciersselectie en naleving van beveiligingsvereisten

4.1.2 Keurt contracten, uitzonderingen en escalaties met betrekking tot leveranciers goed

4.1.3 Houdt toezicht op incidentrespons en besluitvorming wanneer leveranciers niet aan hun verplichtingen voldoen

4.2 IT-supportverlener of interne contactpersoon informatiebeveiliging

4.2.1 Beoordeelt de technische toegang die door leveranciers wordt aangevraagd

4.2.2 Implementeert regels voor toegangsbeheersing, beoordeelt logbestanden en verifieert veilige gegevensverwerking

4.2.3 Beoordeelt bewijs van beveiligingsmaatregelen, certificeringen of auditresultaten, indien van toepassing

[... 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 jaarlijks worden beoordeeld door de algemeen directeur, met betrokkenheid van de IT-supportverlener of leveranciersmanager.

9.2 Het beleid moet ook worden beoordeeld:

9.2.1 na elke significante wijziging in wettelijke, reglementaire of contractuele verplichtingen

9.2.2 na een leveranciersgerelateerd beveiligingsincident of een auditbevinding

9.2.3 bij introductie van nieuwe leverancierscategorieën (bijv. kritieke SaaS-platforms)

9.3 Alle actualisaties moeten:

9.3.1 worden gedocumenteerd met versiehistorie en onderbouwing

9.3.2 worden goedgekeurd door de algemeen directeur

9.3.3 worden gecommuniceerd aan relevante interne medewerkers en leveranciersmanagers

9.3.4 samen met eerdere versies worden opgeslagen overeenkomstig P14S – Gegevensbewarings- en vernietigingsbeleid

10. Gerelateerde beleidslijnen en samenhang

10.1 De doeltreffendheid van dit beleid is afhankelijk van afstemming met de volgende mkb-beleidslijnen voor informatiebeveiliging:

10.1.1 P2S – Beleid inzake governancerollen en -verantwoordelijkheden: wijst verantwoordelijkheid toe voor toezicht op leveranciers en handhaving van contracten.

10.1.2 P4S – Beleid inzake toegangsbeheersing: biedt regels voor toegangsbeperking die moeten worden toegepast wanneer leveranciers systeemtoegang krijgen.

10.1.3 P17S – Beleid inzake gegevensbescherming en privacy: waarborgt dat leveranciers die persoonsgegevens verwerken, voldoen aan beginselen inzake gegevensbescherming en wettelijke vereisten.

10.1.4 P14S – Gegevensbewarings- en vernietigingsbeleid: is van toepassing op alle gegevens of registraties die met leveranciers worden gedeeld of door leveranciers worden opgeslagen en regelt veilige vernietiging na contractbeëindiging.

10.1.5 P30S – Incidentresponsbeleid (P30): definieert hoe moet worden gereageerd wanneer een leverancier een beveiligingsincident veroorzaakt of daarbij betrokken is, met inbegrip van escalatie- en procedures voor bewijsverzameling.

10.2 Deze beleidslijnen waarborgen gezamenlijk dat leveranciersrisico gedurende de volledige contractlevenscyclus wordt beheerst.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001

11.1.1 Clausule 8.1 – Vereist de implementatie van operationele beheersmaatregelen, waaronder die voor relaties met derde partijen en leveranciers.

11.2 ISO/IEC 27002

11.2.1 Beheersmaatregel 5.19 – Waarborgt dat beveiligingsmaatregelen voor leveranciers zijn afgestemd op de vereisten van de organisatie.

11.2.2 Beheersmaatregel 5.20 – Vereist formele overeenkomsten die beveiligingsvoorwaarden, verantwoordelijkheden en verplichtingen bij inbreuken afdekken.

11.2.3 Beheersmaatregel 5.21 – Beheerst wijzigingen in leveranciersdiensten die de risicopositie op het gebied van informatiebeveiliging kunnen beïnvloeden.

11.2.4 Beheersmaatregel 5.22 – Vereist monitoring en beoordeling van leveranciersdiensten en naleving.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-9 – Regelt de verwerving van externe systemen en diensten en vereist risicobeoordelingen en duidelijk vastgelegde verwachtingen.

11.3.2 SA-10 – Beheerst configuratie- en wijzigingsprocedures waarbij door derde partijen beheerde systemen betrokken zijn.

11.3.3 CA-3 – Vereist interconnectieovereenkomsten voor systemen waarbij externe entiteiten zijn betrokken.

11.3.4 PS-7 – Specificeert screening en verantwoordingsplicht voor extern personeel.

11.4 AVG (2016/679)

11.4.1 Artikel 28 – Vereist verwerkersovereenkomsten met leveranciers die optreden als verwerker.

11.4.2 Artikel 32 – Verplicht passende technische en organisatorische beveiligingsmaatregelen voor alle externe gegevensverwerkers.

11.5 EU NIS2-richtlijn (2022/2555)

11.5.1 Artikel 21(2)(a), (b), (i) – Verplicht ICT-risicobeheer in de toeleveringsketen en beheersmaatregelen voor derde partijen.

11.5.2 Artikel 23(1) – Vereist gedocumenteerd toezicht op diensten van derde partijen voor essentiële en belangrijke entiteiten.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 5(1) – Vereist een ICT-risicobeheerkader dat alle kritieke aanbieders van derde partijen omvat.

11.6.2 Artikel 5(2) – Stelt contractuele en operationele beheersmaatregelen vast voor afhankelijkheden van ICT-diensten.

11.6.3 Artikel 28(1), (2) – Stelt toezichtregels vast voor ICT-risico van derde partijen in de financiële sector.

11.7 COBIT 2019

11.7.1 APO10 – "Manage Suppliers" beschrijft sourcingbeheersmaatregelen en verwachtingen voor relatiebeheer.

11.7.2 APO12 – "Manage Risk" integreert leveranciersrisico in de governancestructuur voor organisatierisico's.

11.7.3 DSS05 – "Manage Security Services" is van toepassing op beheerde derde partijen en uitbestede dienstverleners.