					Voer hier de naam van de geregistreerde rechtspersoon in						
Documentnummer: P26					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 planning en beheersing: vereist formele beheersmaatregelen voor diensten van derden die impact hebben op het ISMS
ISO/IEC 27002:2022	Beheersmaatregelen 5.19–5.22	Beleid en procedures voor leveranciersrelaties; beheer van leveranciersrisico's; beheer van dienstverlening door leveranciers; monitoring en beoordeling van leveranciers
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Externe systeemdiensten; configuratiebeheer door ontwikkelaars; systeemkoppelingen; beveiliging van personeel van derde partijen
AVG	Artikelen 28, 32, 33	Verplichtingen van de verwerker; beveiliging van de verwerking; melding van een inbreuk in verband met persoonsgegevens
NIS2-richtlijn	Artikel 21(2)(e–f)	Risicogebaseerd leveranciersmanagement en beveiligingstoezicht
DORA	Artikelen 28, 30	ICT-risico van derde partijen; toezicht op kritieke ICT-dienstverleners van derde partijen
COBIT 2019	BAI05, DSS02, MEA03	Organisatorische verandercapaciteit beheren; serviceverzoeken en incidenten beheren; naleving monitoren, evalueren en beoordelen

1. Doel

1.1 Dit beleid definieert de informatiebeveiligingseisen voor het aangaan, beheren en onderhouden van veilige relaties met leveranciers en dienstverleners van derde partijen.

1.2 Het waarborgt dat alle leveranciers met toegang tot gegevens, systemen of infrastructuur van de organisatie gedurende de volledige levenscyclus van de dienstverlening zijn onderworpen aan stringente beveiligingsmaatregelen, contractuele waarborgen en doorlopend toezicht.

1.3 Dit beleid ondersteunt ISO/IEC 27001 Bijlage A, beheersmaatregelen 5.19 tot en met 5.22, door beveiligingseisen te verankeren in inkoop, onboarding, due diligence, contractbeheer, servicemonitoring en beëindigingsprocessen.

2. Reikwijdte

2.1 Dit beleid is van toepassing op:

2.1.1 alle leveranciers, contractanten, cloudproviders en dienstverlenende organisaties van derde partijen die informatieactiva van de organisatie verwerken of daartoe toegang hebben

2.1.2 alle interne rollen die betrokken zijn bij leveranciersbeoordeling, onboarding, contractering, risicobeheer, monitoring of beëindiging

2.1.3 alle leveranciersrelaties die toegang tot gevoelige gegevens omvatten, integratie met productieomgevingen vereisen of ondersteuning bieden aan kritieke bedrijfsfuncties

2.2 Dit beleid omvat, waar van toepassing, zowel directe leveranciers als hun onderaannemers en ziet tevens op software van derden, infrastructuur, ondersteuning en beheerde diensten.

3. Doelstellingen

3.1 Waarborgen dat leveranciersrisico's gedurende de volledige levenscyclus van de relatie consistent worden geïdentificeerd, beoordeeld en gemitigeerd.

3.2 Gestandaardiseerde beveiligingseisen opnemen in alle leverancierscontracten, met inbegrip van meldverplichtingen bij inbreuken, auditrechten en verantwoordelijkheden op het gebied van gegevensbescherming.

3.3 Formele due diligence en gedocumenteerde risicobeoordelingen vereisen voordat nieuwe leveranciers worden ingeschakeld of dienstverleningsovereenkomsten met een hoog risico worden verlengd.

3.4 Mechanismen vaststellen voor continue nalevingsmonitoring van leveranciers, waaronder prestatiebeoordelingen, audits en incidentescalatie.

3.5 Wijzigingen in leveranciersdiensten beheersen en veilige offboarding en teruggave of vernietiging van gegevens afdwingen bij beëindiging.

3.6 Beveiligingsmaatregelen voor derde partijen afstemmen op toepasselijke wet- en regelgeving en contractuele verplichtingen, waaronder de AVG, NIS2, DORA en ISO/IEC 27001.

4. Rollen en verantwoordelijkheden

4.1 Chief Information Security Officer (CISO)

4.1.1 Is eigenaar van dit beleid en waarborgt de afstemming ervan op de algehele ISMS-, risicobeheer- en compliancestrategie.

4.1.2 Keurt classificatieniveaus voor leveranciers, uitkomsten van beveiligingsbeoordelingen en uitzonderingen met een hoog risico goed.

4.1.3 Neemt deel aan de escalatie van ernstige leveranciersincidenten en aan contractonderhandelingen voor kritieke diensten.

4.2 Inkoop en leveranciersmanagement

4.2.1 Zorgt ervoor dat alle nieuwe en verlengde leverancierscontracten goedgekeurde beveiligings- en gegevensbeschermingsclausules bevatten.

4.2.2 Beheert het centrale leveranciersregister en stemt met Juridische Zaken en Compliance af over documentatie inzake risico's van derde partijen.

4.2.3 Initieert onboardingprocessen en zorgt voor afstemming met beveiligingsbeoordelingen voorafgaand aan contractsluiting.

[... 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 Dit beleid moet ten minste jaarlijks worden herzien, of eerder in geval van:

9.1.1 materiële wijzigingen in de inkoopstrategie of het leverancierslandschap

9.1.2 actualisaties van wettelijke of regelgevende kaders (bijv. DORA, AVG)

9.1.3 majeure incidenten bij derde partijen, datalekken of tekortkomingen bij audits

9.1.4 bevindingen uit risicobeoordelingen of van externe certificerende instellingen

9.2 Het herzieningsproces valt onder gezamenlijk eigenaarschap van de CISO en de functies Inkoop, Juridische Zaken en Compliance en Risicobeheer.

9.3 Alle beleidsrevisies moeten worden gedocumenteerd in het ISMS-documentenregister, onder versiebeheer worden geplaatst en via governancekanalen voor leveranciers en bewustwordingsprogramma's voor medewerkers aan relevante stakeholders worden gecommuniceerd.

9.4 Vervangen versies moeten ten minste drie jaar worden gearchiveerd ten behoeve van traceerbaarheid en wettelijke naleving.

10. Gerelateerde beleidslijnen en samenhang

10.1 P1 – Informatiebeveiligingsbeleid. Legt de overkoepelende verplichting vast om alle activiteiten van de organisatie te beveiligen, inclusief afhankelijkheden van leveranciers en externe dienstverleners van derde partijen.

10.2 P6 – Beleid inzake risicobeheer. Geeft richting aan de identificatie, beoordeling en mitigatie van risico's die samenhangen met relaties met derde partijen, waaronder overgenomen of systemische risico's binnen leveranciersketens.

10.3 P17 – Beleid inzake gegevensbescherming en privacy. Is van toepassing op alle leveranciers die persoonsgegevens verwerken en vereist passende contractuele bepalingen, waarborgen voor doorgifte en privacy-by-design-principes.

10.4 P4 – Beleid inzake toegangsbeheer. Regelt hoe personeel van derde partijen toegang krijgt tot systemen van de organisatie, met handhaving van rolgebaseerde rechten, sessiebeheer en intrekkingsprocedures.

10.5 P22 – Beleid voor logging en monitoring. Vereist dat toegang van leveranciers tot systemen wordt gemonitord, gelogd en beoordeeld, met name in omgevingen waar geprivilegieerde of datagerichte activiteiten plaatsvinden.

10.6 P30 – Incidentresponsbeleid (P30). Definieert escalatieprocedures en vereisten voor rapportage van inbreuken voor door leveranciers veroorzaakte beveiligingsgebeurtenissen of gezamenlijke onderzoeken waarbij systemen van derde partijen zijn betrokken.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001: Clausule 8.1 – Operationele planning en beheersing: vereist formele beheersmaatregelen voor diensten van derden die impact hebben op het ISMS.

11.2 ISO/IEC 27002:2022 – Beheersmaatregelen 5.19 tot en met 5.22:

11.2.1 Bijlage A, beheersmaatregel 5.19 – Beleid en procedures voor leveranciersrelaties: schrijft beheersmaatregelen voor het beheren van interacties met leveranciers.

11.2.2 Bijlage A, beheersmaatregel 5.20 – Beheer van leveranciersrisico's: richt zich op identificatie, beoordeling en doorlopend toezicht op de risicopositie van leveranciers op het gebied van informatiebeveiliging.

11.2.3 Bijlage A, beheersmaatregel 5.21 – Beheer van dienstverlening door leveranciers: vereist afstemming van prestaties en beveiliging op contractuele verwachtingen.

11.2.4 Bijlage A, beheersmaatregel 5.22 – Monitoring en beoordeling van leveranciers: benadrukt de noodzaak van doorlopende validatie en herbeoordeling van de naleving door derde partijen.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SA-9 – Externe systeemdiensten: definieert beveiligings- en risicovereisten voor systemen die door externe entiteiten worden geëxploiteerd.

11.3.2 SA-10 – Configuratiebeheer door ontwikkelaars: is van toepassing wanneer derde partijen software of omgevingen leveren.

11.3.3 CA-3 – Systeemkoppelingen: vereist toezicht op en afspraken over gegevensstromen tussen systemen van verschillende entiteiten.

11.3.4 PS-7 – Beveiliging van personeel van derde partijen: waarborgt dat contractanten en personeel van leveranciers passend worden gescreend en gevolgd.

11.4 AVG (2016/679):

11.4.1 Artikel 28 – Verplichtingen van de verwerker: vereist schriftelijke overeenkomsten met externe gegevensverwerkers, inclusief technische en organisatorische maatregelen (TOM's).

11.4.2 Artikel 32 – Beveiliging van de verwerking: verplicht tot passende waarborgen door zowel verwerkingsverantwoordelijken als verwerkers.

11.4.3 Artikel 33 – Melding van een inbreuk in verband met persoonsgegevens: vereist tijdige melding door leveranciers in geval van een inbreuk.

11.5 NIS2-richtlijn (2022/2555):

11.5.1 Artikel 21(2)(e–f): vereist risicogebaseerd leveranciersmanagement en beveiligingstoezicht, met name in digitale toeleveringsketens van essentiële en belangrijke entiteiten.

11.6 DORA (2022/2554):

11.6.1 Artikel 28 – ICT-risico van derde partijen: legt verplichtingen op ten aanzien van risicobeoordeling, contractuele beveiligingsvoorwaarden en exitstrategieën voor aanbieders van financiële diensten.

11.6.2 Artikel 30 – Toezicht op kritieke ICT-dienstverleners van derde partijen: stelt verscherpte eisen aan monitoring en toezicht op belangrijke leveranciers.

11.7 COBIT 2019:

11.7.1 BAI05 – Organisatorische verandercapaciteit beheren: waarborgt dat leveranciersovergangen op beheerste en veilige wijze plaatsvinden.

11.7.2 DSS02 – Serviceverzoeken en incidenten beheren: is van toepassing op door leveranciers gemelde issues en integratie met incidentafhandeling.

11.7.3 MEA03 – Naleving monitoren, evalueren en beoordelen: versterkt de meting van leverancierspresta ties en nalevingsmonitoring.