					Voer hier de naam van de geregistreerde rechtspersoon in						
Documentnummer: PII17					Documenttitel: **Beleid voor PIMS-gedocumenteerde informatie en beheer van bewijsmateriaal**						
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 / beheersmaatregel / artikel	Toepasselijkheid	Dekkingstype	Opmerking
ISO/IEC 27701:2025	Clause 6.1.3	Both	Supporting	SoA-gedocumenteerde informatie
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	PIMS-gedocumenteerde informatie
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Beheersing van operationeel bewijsmateriaal
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Bewijsmateriaal voor monitoring
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Auditbewijsmateriaal
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Bewijsmateriaal voor directiebeoordeling
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Bewijsmateriaal voor non-conformiteit en corrigerende maatregelen
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Verwerkingsregistraties van verwerkingsverantwoordelijken
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Bewijsmateriaal voor verwerkersovereenkomsten en instructies
ISO/IEC 27701:2025	Annex A.3.14	Both	Primary	Bescherming van registraties
GDPR	Article 5(2)	Controller	Supporting	Bewijsmateriaal voor verantwoordingsplicht
GDPR	Article 24	Controller	Supporting	Maatregelen en bewijsmateriaal van de verwerkingsverantwoordelijke
GDPR	Article 28	Both	Supporting	Documentatie van verwerkers
GDPR	Article 30	Both	Supporting	Verwerkingsregistraties
GDPR	Article 32	Both	Supporting	Bescherming van bewijsmateriaal
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Bewijsmateriaal voor privacynaleving
ISO/IEC 29151:2022	Clause 18.1.4	Both	Supporting	Bescherming van registraties
ISO/IEC 27001:2022	Clause 7.5	Both	Supporting	Beheersing van gedocumenteerde informatie

ISO/IEC 27002:2022	Control 5.33	Both	Supporting	Bescherming van registraties
ISO/IEC 27002:2022	Control 5.34	Both	Supporting	Bescherming van privacy en PII

1. Reikwijdte

1.1 Dit beleid definieert verplichte eisen voor het opstellen, goedkeuren, versioneren, beschermen, bewaren, opvragen, vertalen, intrekken en onderbouwen van PIMS-gedocumenteerde informatie met bewijsmateriaal.

1.2 Dit beleid is van toepassing op PIMS-beleidsdocumenten, registers, gedocumenteerde goedkeuringen, bewijsregistraties, auditbewijsmateriaal, registraties van directiebeoordelingen, bewijsmateriaal voor corrigerende maatregelen en beheerste vertalingen die worden gebruikt om PIMS-conformiteit aan te tonen.

1.3 Dit beleid is van toepassing in contexten van verwerkingsverantwoordelijken, gezamenlijke verwerkingsverantwoordelijken, verwerkers en subverwerkers.

1.4 Dit beleid creëert geen afzonderlijk register voor documentbeheersing. Bewijsmateriaal voor beheersing van gedocumenteerde informatie wordt onderhouden via de canonieke PIMS-bewijsobjecten REG01 tot en met REG12, waarbij REG03 en REG12 worden gebruikt voor toepasselijkheid van beheersmaatregelen, audit, non-conformiteit, corrigerende maatregelen en bewijsmateriaal voor verbetering.

2. Doel

2.1 Het doel van dit beleid is te waarborgen dat PIMS-gedocumenteerde informatie juist, beheerst en toegankelijk is voor geautoriseerde gebruikers, beschermd is tegen ongeautoriseerde wijziging of openbaarmaking, wordt bewaard ten behoeve van auditeerbaarheid en wordt ingetrokken wanneer zij verouderd is.

2.2 Dit beleid ondersteunt de gereedheid voor certificering door te waarborgen dat bewijsmateriaal dat nodig is om PIMS-conformiteit aan te tonen, kan worden gevonden, geverifieerd, opgehaald en gekoppeld aan toepasselijke beleidsdocumenten, beheersmaatregelen, verwerkingsactiviteiten, risico's, audits en corrigerende maatregelen.

3. Doelstellingen

3.1 De doelstellingen van dit beleid zijn:

3.1.1 eisen voor beheersing van PIMS-gedocumenteerde informatie definiëren;

3.1.2 de integriteit van bewijsmateriaal in REG01 tot en met REG12 handhaven;

3.1.3 waarborgen dat goedkeuring van beleid en bewijsmateriaal traceerbaar is;

3.1.4 waarborgen dat versiehistorie en intrekkingsbesluiten worden gedocumenteerd;

3.1.5 PIMS-bewijsmateriaal koppelen aan de Verklaring van Toepasselijkheid en beleidsmappingen;

3.1.6 de toegang tot PIMS-documenten en bewijsregistraties beheersen;

3.1.7 meertalig versiebeheer van beleid en bewijsmateriaal ondersteunen;

3.1.8 tijdig opvragen van auditbewijsmateriaal mogelijk maken;

3.1.9 onnodige bureaucratie rond documentbeheersing voorkomen;

3.1.10 auditklare registraties behouden ten behoeve van certificering, assurance richting klanten en voortdurende verbetering.

4. Beleidsverklaringen

4.1 Beheersing van PIMS-gedocumenteerde informatie

4.1.1 [All] Privacy Lead / PIMS Manager MOET vóór de initiële PIMS-publicatie en vervolgens elk kwartaal een index van PIMS-gedocumenteerde informatie bijhouden in REG12.

4.1.2 [All] Process Owner / Business Owner MOET vóór aanvang van de verwerkingsactiviteit en vervolgens jaarlijks in REG02 vaststellen welke gedocumenteerde informatie vereist is voor elke eigen PII-verwerkingsactiviteit.

4.1.3 [All] Privacy Lead / PIMS Manager MOET vóór elke beleidsrelease en binnen 15 werkdagen na elke wezenlijke wijziging in de toepasselijkheid van beheersmaatregelen toepasselijke PIMS-beleidsdocumenten, beheersmaatregelen en bewijsverplichtingen koppelen aan REG03.

4.1.4 [All] Privacy Lead / PIMS Manager MOET een toegangsniveau en classificatie van de gevoeligheid van bewijsmateriaal toewijzen aan elke categorie PIMS-gedocumenteerde informatie in REG12 voordat de categorie wordt gebruikt.

4.2 Opstelling, goedkeuring, versionering en publicatie

4.2.1 [All] Privacy Lead / PIMS Manager MOET vóór publicatie van PIMS-gedocumenteerde informatie een documentidentificatie, eigenaar, versienummer, goedkeuringsstatus, ingangsdatum en beoordelingsdatum vastleggen in REG12.

4.2.2 [All] Top Management MOET kernbeleidsdocumenten van het PIMS en wezenlijke beleidswijzigingen vóór publicatie goedkeuren in REG12.

4.2.3 [All] Privacy Lead / PIMS Manager MOET PIMS-sjablonen voor bewijsmateriaal of ingebedde registeronderdelen vóór operationeel gebruik goedkeuren in REG12.

4.2.4 [All] Privacy Lead / PIMS Manager MOET vóór vrijgave van bijgewerkte PIMS-gedocumenteerde informatie de versiehistorie en de wijzigingsmotivering vastleggen in REG12.

4.2.5 [All] Privacy Lead / PIMS Manager MOET communicatie over goedgekeurde wijzigingen in PIMS-gedocumenteerde informatie binnen 30 dagen na publicatie vastleggen in REG11.

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

9. Uitzonderingen

9.1.1 [All] Process Owner / Business Owner MOET uitzonderingen op gedocumenteerde informatie of op beheersing van bewijsmateriaal aanvragen in REG12 voordat van dit beleid wordt afgeweken.

9.1.2 [All] Privacy Lead / PIMS Manager MOET elke uitzondering op gedocumenteerde informatie of beheersing van bewijsmateriaal binnen 10 werkdagen na aanvraag beoordelen in REG12.

9.1.3 [All] Data Protection Officer / Privacy Advisor MOET advies vastleggen in REG12 vóór goedkeuring van elke uitzondering die betrekking heeft op openbaarmaking van PII-bewijsmateriaal, vertaalafwijkingen, bewaarconflicten of beperkingen van auditbewijsmateriaal.

9.1.4 [All] Top Management MOET uitzonderingen op gedocumenteerde informatie die langer dan 30 dagen duren of gevolgen hebben voor certificering, verwerking met hoog risico of externe assurance, goedkeuren in REG12 voordat de uitzondering van kracht wordt.

9.1.5 [All] Privacy Lead / PIMS Manager MOET voor elke goedgekeurde uitzondering op gedocumenteerde informatie of beheersing van bewijsmateriaal in REG12 een vervaldatum vaststellen die niet meer dan 90 dagen bedraagt.

9.1.6 [All] Privacy Lead / PIMS Manager MOET elke uitzondering op gedocumenteerde informatie of beheersing van bewijsmateriaal binnen vijf werkdagen na het verstrijken ervan sluiten of opnieuw beoordelen in REG12.

10. Handhaving

10.1.1 [All] Privacy Lead / PIMS Manager MOET ontbrekende, onjuiste, onbeheerde, verouderde of niet-opvraagbare PIMS-gedocumenteerde informatie binnen vijf werkdagen na identificatie als non-conformiteit vastleggen in REG12.

10.1.2 [All] Privacy Lead / PIMS Manager MOET publicatie van PIMS-gedocumenteerde informatie voorkomen wanneer vereist bewijsmateriaal over goedkeuring, versie, eigenaar of ingangsdatum ontbreekt in REG12.

10.1.3 [All] Process Owner / Business Owner MOET indiening van verwerkingsbewijsmateriaal voor audits voorkomen wanneer vereist bewijsmateriaal over eigenaar, datum, status of goedkeuring ontbreekt in REG02.

10.1.4 [All] System Owner / Application Owner MOET ongeautoriseerde toegang tot repositories met PIMS-gedocumenteerde informatie verwijderen en de verwijdering binnen één werkdag na identificatie vastleggen in REG12.

10.1.5 [All] Internal Audit / Compliance Reviewer MOET de doeltreffendheid van corrigerende maatregelen voor non-conformiteiten met betrekking tot gedocumenteerde informatie verifiëren in REG12 bij de eerstvolgende geplande audit of binnen 60 dagen na sluiting, afhankelijk van wat zich het eerst voordoet.

11. Beoordeling en onderhoud

11.1.1 [All] Privacy Lead / PIMS Manager MOET dit beleid jaarlijks en binnen 30 dagen na een wezenlijke wijziging in eisen voor PIMS-gedocumenteerde informatie beoordelen.

11.1.2 [All] Privacy Lead / PIMS Manager MOET dit beleid binnen 30 dagen na een belangrijke auditbevinding, certificeringsnon-conformiteit, wijziging van repositoryplatform of wijziging van het proces voor meertalige publicatie beoordelen.

11.1.3 [All] Data Protection Officer / Privacy Advisor MOET privacyrelevante wijzigingen in dit beleid vóór goedkeuring beoordelen in REG12.

11.1.4 [All] Top Management MOET wezenlijke wijzigingen in dit beleid vóór publicatie goedkeuren in REG12.

11.1.5 [All] Privacy Lead / PIMS Manager MOET communicatie over goedgekeurde wijzigingen in dit beleid binnen 30 dagen na publicatie vastleggen in REG11.

12. Gerelateerde beleidsdocumenten

12.1 Dit beleid wordt ondersteund door de volgende gerelateerde beleidsdocumenten:

12.2 PII01 - Beleid voor het privacy-informatiemanagementsysteem

12.3 PII02 - Beleid voor privacyrollen, verantwoordelijkheden en verantwoordingsplicht

12.4 PII03 - Beleid voor PII-verwerkingsinventaris en rechtsgrondslag

12.5 PII04 - Beleid voor privacyverklaring en transparantie

12.6 PII05 - Beleid voor toestemmings- en voorkeurenbeheer

12.7 PII06 - Beleid voor beheer van rechten van betrokkenen

12.8 PII07 - Beleid voor privacyrisicobeoordeling en DPIA

12.9 PII08 - Beleid voor privacy by design en privacy by default

12.10 PII09 - Beleid voor verzameling, gebruik, verstrekking en delen van PII

12.11 PII10 - Beleid voor bewaring, verwijdering en afvoer van PII

12.12 PII11 - Beleid voor juistheid en kwaliteit van PII

12.13 PII12 - Beleid voor privacybeheer van verwerkers, subverwerkers en derde partijen

12.14 PII13 - Beleid voor internationale doorgifte van PII

12.15 PII14 - Beleid voor PII-beveiliging en toegangscontrole

12.16 PII15 - Beleid voor incident- en inbreukbeheer met betrekking tot PII

12.17 PII16 - Beleid voor privacytraining, bewustwording en competentie

12.18 PII18 - Beleid voor PIMS-monitoring, audits en verbetering

13. Referentienormen en -raamwerken

13.1 Dit beleid is gekoppeld aan de volgende normen en regelgeving. De mapping licht toe hoe het beleid de aangehaalde eisen ondersteunt en identificeert de interne clausules die deze implementeren of ondersteunen.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.3** - Gekoppeld aan het onderhouden van de PIMS-Verklaring van Toepasselijkheid, registraties van toepasselijkheid van beheersmaatregelen en koppeling tussen beleid en bewijsmateriaal. Addressed by clauses [4.1.3; 4.3.3; 6.1.3; 7.1.2].

13.2.2 **Clause 7.5** - Gekoppeld aan identificatie van gedocumenteerde informatie, goedkeuring, versiebeheer, toegang, opvraging, behoud, intrekking, koppeling van vertaalversies en bewaarmetadata. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.5; 4.4.1; 4.4.2; 4.4.4; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.1; 4.6.2; 4.6.3; 4.6.4].

13.2.3 **Clause 8.1** - Gekoppeld aan bewijsmateriaal voor operationele planning en beheersing voor verwerkingsregistraties, sjablonen voor bewijsmateriaal, kwaliteit van operationeel bewijsmateriaal en extern aangeleverd bewijsmateriaal. Addressed by clauses [4.1.2; 4.2.3; 4.3.2; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1** - Gekoppeld aan het onderhouden van gedocumenteerd bewijsmateriaal voor meting, prestaties van opvraging, lacunes in bewijsmateriaal, vertaalafwijkingen en voltooiing van toegangsbeoordelingen voor repositories. Addressed by clauses [8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6].

13.2.5 **Clause 9.2** - Gekoppeld aan opvraging van auditbewijsmateriaal, auditsteekproeven, traceerbaarheid van auditbewijsmateriaal en auditbevindingen met betrekking tot beheersing van gedocumenteerde informatie. Addressed by clauses [4.3.4; 4.4.4; 6.1.3; 8.1.3; 10.1.5].

13.2.6 **Clause 9.3** - Gekoppeld aan bewijsmateriaal voor directiebeoordeling, behandeling van beheersing van gedocumenteerde informatie in directiebeoordelingen en beoordeling door Top Management van prestaties van beheersing van bewijsmateriaal. Addressed by clauses [6.1.2; 8.1.1; 8.1.2; 11.1.4].

13.2.7 **Clause 10.2** - Gekoppeld aan non-conformiteiten met betrekking tot gedocumenteerde informatie, corrigerende maatregelen, afhandeling van uitzonderingen, sluiting en verificatie van doeltreffendheid. Addressed by clauses [4.3.4; 6.1.4; 9.1.1; 9.1.2; 9.1.4; 9.1.5; 9.1.6; 10.1.1; 10.1.5].

13.2.8 **Annex A.1.2.9** - Gekoppeld aan verwerkingsregistraties van verwerkingsverantwoordelijken, verantwoordingsregistraties, kwaliteit van verwerkingsbewijsmateriaal en bewaring van bewijsmateriaal ter ondersteuning van verplichtingen van verwerkingsverantwoordelijken. Addressed by clauses [4.1.2; 4.3.2; 4.5.1; 7.1.3].

13.2.9 **Annex A.2.2.2** - Gekoppeld aan verwerkersovereenkomst, klantinstructie, extern aangeleverd bewijsmateriaal en beheersing van bewijsmateriaal over verwerkersrelaties. Addressed by clauses [5.1.7; 7.1.4].

13.2.10 **Annex A.3.14** - Gekoppeld aan bescherming van PIMS-registraties tegen verlies, ongeautoriseerde wijziging, ongeautoriseerde toegang, ongeautoriseerde vrijgave en onjuiste verwijdering. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.2; 4.5.4; 4.5.5; 10.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Gekoppeld aan bewijsmateriaal voor verantwoordingsplicht, traceerbaarheid van bewijsmateriaal, opvraging van bewijsmateriaal, registraties van non-conformiteiten en auditklare registraties om naleving aan te tonen. Addressed by clauses [4.1.1; 4.3.2; 4.3.3; 4.4.4; 4.5.4; 6.1.3; 8.1.3; 10.1.1].

13.3.2 **Article 24** - Gekoppeld aan governancebewijsmateriaal van verwerkingsverantwoordelijken, goedkeuringsregistraties, beleidsbeheersing, maatregelen voor verantwoordingsplicht, gedocumenteerde beoordeling en toezicht door Top Management. Addressed by clauses [4.2.2; 4.3.3; 6.1.2; 9.1.4; 11.1.4].

13.3.3 **Article 28** - Gekoppeld aan documentatie over verwerkers en subverwerkers, bewijsmateriaal voor klantinstructies, extern aangeleverd procesbewijsmateriaal en beheersing van openbaarmaking van bewijsmateriaal. Addressed by clauses [4.4.5; 5.1.7; 7.1.4].

13.3.4 **Article 30** - Gekoppeld aan bewijsmateriaal voor verwerkingsregistraties, kwaliteitseisen voor bewijsmateriaal, verwijzingen naar verwerkingsactiviteiten en metadata over eigenaar/status van verwerkingsbewijsmateriaal. Addressed by clauses [4.1.2; 4.3.2; 7.1.3; 10.1.3].

13.3.5 **Article 32** - Gekoppeld aan bescherming van bewijsrepositories, toegangsbeperkingen, toegangsgoedkeuringen, beoordeling van repositorybescherming en verwijdering van ongeautoriseerde toegang. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Gekoppeld aan bewijsmateriaal voor privacynaleving, opvraging van auditbewijsmateriaal, traceerbaarheid van bewijsmateriaal, ondersteuning van onafhankelijke beoordeling en bewijsmateriaal voor corrigerende maatregelen. Addressed by clauses [4.3.3; 4.4.4; 4.6.3; 6.1.3; 8.1.3; 10.1.5].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.1.4** - Gekoppeld aan bescherming van PII-gerelateerde registraties, behoud van registraties en controles voor toegang tot en verwijdering uit bewijsrepositories. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.5.2; 4.5.5; 10.1.4].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 7.5** - Gekoppeld aan identificatie van gedocumenteerde informatie, goedkeuring, beschikbaarheid, bescherming, versiebeheer, bewaring, verwijdering en beheersing van extern vereiste gedocumenteerde informatie. Addressed by clauses [4.1.1; 4.2.1; 4.2.4; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.6.4].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.33 - Gekoppeld aan bescherming van PIMS-registraties tegen verlies, vernietiging, vervalsing, ongeautoriseerde toegang, ongeautoriseerde vrijgave en onjuiste verwijdering. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.7.2 Control 5.34 - Gekoppeld aan bescherming van privacy en PII in gedocumenteerde informatie, bewijsrepositories, openbaarmakingen en registraties met toegangscontrole. Addressed by clauses [4.1.4; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 6.1.5].