					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: PII14					Documenttitel: **Beleid inzake PII-beveiliging en toegangscontrole**							
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	Clause / Control / Article	Toepasselijkheid	Dekkingssoort	Opmerking
ISO/IEC 27701:2025	Clause 6.1.3; Clause 8.1	Both	Primary	Planning en uitvoering van PII-beveiligingsmaatregelen
ISO/IEC 27701:2025	Clause 7.5; Clause 9.1; Clause 10.2	Both	Supporting	Bewijsmateriaal, monitoring en corrigerende maatregelen
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9	Both	Primary	Identiteit en toegangsrechten voor PII-verwerking
ISO/IEC 27701:2025	Annex A.3.22; Annex A.3.23	Both	Primary	Endpointbescherming en veilige authenticatie
ISO/IEC 27701:2025	Annex A.3.25; Annex A.3.26	Both	Primary	Logging en cryptografische bescherming
ISO/IEC 27701:2025	Annex A.3.28; Annex A.3.29	Both	Supporting	Applicatiebeveiliging en beveiligde architectuur
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.15; Annex A.3.16	Both	Supporting	Bescherming en beoordeling van registraties
GDPR	Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32	Both	Primary	Beveiliging, verantwoordingsplicht en beheersmaatregelen voor verwerkers
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Integratie van ISMS-beheersmaatregelen
ISO/IEC 27002:2022	Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Implementatierichtlijnen voor beveiligingsmaatregelen
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Beginselen voor informatiebeveiliging en naleving van privacyverplichtingen
ISO/IEC 29151:2022	Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2;	Both	Supporting	Beveiligingsmaatregelen voor PII-bescherming

	Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4			

1. Reikwijdte

1.1 Dit beleid definieert PII-specifieke beveiligings- en toegangscontrole-eisen voor systemen, toepassingen, diensten, apparaten, cloudomgevingen en operationele processen die PII opslaan, verzenden, verwerken, raadplegen, beheren of beschermen.

1.2 Dit beleid is van toepassing op contexten van verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker en subverwerker waarin de organisatie beveiligingsmaatregelen voor PII-verwerking bepaalt, uitvoert, ondersteunt of daarop vertrouwt.

1.3 Dit beleid omvat de volgende domeinen van PII-beveiligingsmaatregelen:

1.3.1 PII-beveiligingsbaseline en integratie met bestaande informatiebeveiligingsbeleidstukken;

1.3.2 toegangscontrole;

1.3.3 authenticatie;

1.3.4 geprivilegieerde toegang;

1.3.5 encryptie en veilige opslag;

1.3.6 logging en monitoring;

1.3.7 beveiligde configuratie en kwetsbaarhedenbeheer;

1.3.8 endpoint- en cloudtoegangscontroles;

1.3.9 koppeling van bewijsmateriaal via REG02, REG08, REG10 en REG12.

1.4 Dit beleid vervangt geen volledig informatiebeveiligingsmanagementsysteem, netwerkbeveiligingsbeleid, beleid inzake veilige ontwikkeling, back-upbeleid, endpointbeleid, cloudbeveiligingsbeleid, cryptografische standaard, procedure voor kwetsbaarhedenbeheer of procedure voor incidentrespons.

1.5 Waar dergelijke beleidstukken al bestaan, definieert dit beleid de PII-specifieke koppeling en eisen aan bewijsmateriaal die nodig zijn voor PIMS-assurance.

1.6 Dit beleid dupliceert niet:

1.6.1 eigenaarschap van de PII-verwerkingsinventaris en rechtsgrondslag in PII03;

1.6.2 methodologie voor privacyrisico en DPIA in PII07;

1.6.3 privacy by design-gates in PII08;

1.6.4 regels voor verzameling, gebruik, verstrekking en delen in PII09;

1.6.5 uitvoering van bewaring, verwijdering en afvoer in PII10;

1.6.6 governance van de levenscyclus van verwerkers in PII12;

1.6.7 beheersmaatregelen voor internationale doorgiftemechanismen in PII13;

1.6.8 workflow voor incidenten en inbreuken in PII15;

1.6.9 governance van gedocumenteerde informatie in PII17;

1.6.10 governance voor PIMS-monitoring, audit en verbetering in PII18.

1.7 Voor dit beleid zijn operationele logboeken, uitvoer van beveiligingstools, exporten van toegangsrechtenbeoordelingen, kwetsbaarheidsrapporten en configuratiebewijsmateriaal bronnen van bewijsmateriaal die worden toegevoegd aan, samengevat in of waarnaar wordt verwezen door de canonieke bewijsobjecten.

1.8 Dit zijn geen afzonderlijke PIMS-registers.

2. Doel

2.1 Het doel van dit beleid is te waarborgen dat PII gedurende de verwerking wordt beschermd door passende, op risico afgestemde en auditeerbare beveiligings- en toegangscontroles.

2.2 Dit beleid stelt de organisatie in staat aan te tonen dat PII-beveiligingsmaatregelen worden gepland, geïmplementeerd, beoordeeld, gemonitord en verbeterd via REG02, REG08, REG10 en

REG12 zonder dubbele beveiligingsregisters te creëren of bestaande informatiebeveiligingsbeleidstukken te vervangen.

3. Doelstellingen

3.1 De doelstellingen van dit beleid zijn:

3.1.1 een baseline voor PII-toegangscontrole definiëren voor systemen en verwerkingsactiviteiten;

3.1.2 waarborgen dat authenticatiebeheersmaatregelen passend zijn voor de gevoeligheid en toegangscontext van PII;

3.1.3 beoordelingseisen definiëren voor geprivilegieerde en gewone toegang tot PII;

3.1.4 verwachtingen voor encryptie en veilige opslag van PII in rust, tijdens transport en in relevante cloud- of endpointcontexten definiëren;

3.1.5 verwachtingen voor logging en monitoring definiëren voor toegang tot, wijzigingen in en beheer van PII;

3.1.6 eisen aan bewijsmateriaal voor beveiligde configuratie en kwetsbaarheden definiëren voor systemen die PII verwerken;

3.1.7 verwachtingen voor endpoint- en cloudtoegang definiëren zonder een volledig endpoint- of cloudbeveiligingsbeleid te creëren;

3.1.8 vermoedelijke PII-beveiligingsincidenten koppelen aan REG10 zonder de incidentworkflow te dupliceren;

3.1.9 integreren met bestaande informatiebeveiligingsbeleidstukken waar die beschikbaar zijn;

3.1.10 auditgereed bewijsmateriaal onderhouden met uitsluitend REG02, REG08, REG10 en REG12.

4. Beleidsverklaringen

4.1 PII-beveiligingsbaseline en ISMS-integratie

4.1.1 [Both] The Information Security Lead MOET de PII-beveiligingsbaseline voor elk systeem of elke dienst die PII verwerkt in REG12 definiëren voordat het systeem of de dienst in productie gaat of wezenlijk wijzigt.

4.1.2 [Both] The System Owner / Application Owner MOET de locatie van het geïmplementeerde bewijsmateriaal voor PII-beveiligingsmaatregelen in REG12 registreren voordat op een bestaande informatiebeveiligingsmaatregel wordt vertrouwd voor PIMS-assurance.

4.1.3 [Controller] The Process Owner / Business Owner MOET de PII-gevoeligheid, verwerkingscontext en toegangsbehoefte in REG02 identificeren voordat nieuwe of wezenlijk gewijzigde toegang tot PII wordt aangevraagd.

4.1.4 [Processor] The Vendor / Procurement Owner MOET klantbeveiligingsinstructies, grenzen van klantverantwoordelijkheid en beveiligingsverplichtingen van de verwerker in REG08 registreren voordat verwerkerstoegang tot PII van klanten begint of wezenlijk wijzigt.

4.1.5 [Both] The Privacy Lead / PIMS Manager MOET verifiëren dat PII-beveiligingsbewijsmateriaal is gekoppeld aan REG02, REG08, REG10 of REG12 voordat de verwerkingsactiviteit als PIMS-auditeerbaar wordt aanvaard.

4.2 Baseline voor toegangscontrole

4.2.1 [Both] The System Owner / Application Owner MOET toegang tot PII beperken tot goedgekeurde rollen en geautoriseerde gebruikers die in REG02 of REG12 zijn geregistreerd of traceerbaar zijn voordat toegang wordt geactiveerd.

4.2.2 [Both] The Process Owner / Business Owner MOET het zakelijke doel voor PII-toegang in REG02 of REG12 goedkeuren voordat The System Owner / Application Owner toegang verleent.

4.2.3 [Both] The System Owner / Application Owner MOET gebruikerstoegang tot systemen die PII met hoge impact of gevoelige PII verwerken ten minste elk kwartaal beoordelen en de uitkomst van de beoordeling in REG12 registreren.

4.2.4 [Both] The System Owner / Application Owner MOET gebruikerstoegang tot andere systemen die PII verwerken ten minste jaarlijks beoordelen en de uitkomst van de beoordeling in REG12 registreren.

4.2.5 [Both] The System Owner / Application Owner MOET PII-toegang in REG12 binnen één werkdag verwijderen of wijzigen na rolwijziging, beëindiging, contractafronding of wanneer toegang niet langer vereist is.

4.2.6 [Processor] The Vendor / Procurement Owner MOET in REG08 bevestigen dat verwerkerstoegang tot PII van klanten beperkt is tot gedocumenteerde klantinstructies voordat toegang wordt geactiveerd of gewijzigd.

4.2.7 [Subprocessor] The Vendor / Procurement Owner MOET in REG08 bevestigen dat subverwerkerstoegang tot PII beperkt is tot geautoriseerde subverwerkingsactiviteiten voordat subverwerkerstoegang wordt geactiveerd of gewijzigd.

[... 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 [Both] The Information Security Lead MOET elke uitzondering op een PII-beveiligings- of toegangscontrole-eis in REG12 registreren voordat de uitzondering wordt geactiveerd.

9.1.2 [Both] The Data Protection Officer / Privacy Advisor MOET adviseren over PII-beveiligingsuitzonderingen met een hoger risico in REG12 vóór goedkeuring.

9.1.3 [Both] Top Management MOET PII-beveiligingsuitzonderingen in REG12 goedkeuren vóór activering wanneer de uitzondering PII met hoge impact, gevoelige PII, geprivilegieerde toegang, encryptie, logging of onopgeloste hoog-risicokwetsbaarheden raakt.

9.1.4 [Both] The Information Security Lead MOET de vervaldatum van de uitzondering, compenserende beheersmaatregel en beoordelingsdatum in REG12 definiëren vóór goedkeuring van de uitzondering.

9.1.5 [Both] The System Owner / Application Owner MOET verlopen PII-beveiligingsuitzonderingen in REG12 binnen vijf werkdagen na verloop herstellen, verlengen of sluiten.

9.1.6 [Processor] The Vendor / Procurement Owner MOET beveiligingsuitzonderingen van verwerkers of subverwerkers die PII van klanten raken in REG08 en REG12 registreren vóór aanvaarding.

10. Handhaving

10.1.1 [Both] The Privacy Lead / PIMS Manager MOET non-conformiteiten voor ontbrekend of onvolledig PII-beveiligingsbewijsmateriaal binnen vijf werkdagen na identificatie in REG12 registreren.

10.1.2 [Both] The Information Security Lead MOET eigenaarschap voor herstel van falen van PII-beveiligingsmaatregelen binnen vijf werkdagen na validatie in REG12 toewijzen.

10.1.3 [Both] The System Owner / Application Owner MOET ongeautoriseerde, buitensporige of niet-onderbouwde PII-toegang binnen één werkdag na validatie uitschakelen of beperken en de actie in REG12 registreren.

10.1.4 [Conditional] The Incident Response Coordinator MOET handhavingsmaatregelen binnen één werkdag koppelen aan REG10 wanneer de handhavingskwestie een vermoedelijk of bevestigd PII-incident betreft.

10.1.5 [Both] Top Management MOET herhaalde of hoog-risico PII-beveiligingsnon-conformiteiten in REG12 beoordelen vóór de directiebeoordeling.

11. Beoordeling en onderhoud

11.1.1 [All] The Privacy Lead / PIMS Manager MOET dit beleid samen met The Information Security Lead ten minste jaarlijks beoordelen en de uitkomst van de beoordeling in REG12 registreren.

11.1.2 [Both] The Information Security Lead MOET de PII-beveiligingsbaseline in REG12 binnen 30 dagen beoordelen na een wezenlijke wijziging in technologie, dreiging, audit, incident of regelgeving die PII-beveiliging raakt.

11.1.3 [Both] The System Owner / Application Owner MOET PII-beveiligingsbewijsmateriaal op systeemniveau in REG12 binnen 30 dagen bijwerken na een wezenlijke wijziging in architectuur, toegang, configuratie, kwetsbaarheid of logging.

11.1.4 [Processor] The Vendor / Procurement Owner MOET bewijsmateriaal over PII-beveiligingsverantwoordelijkheden van verwerkers en subverwerkers in REG08 binnen 30 dagen beoordelen na een wezenlijke wijziging van dienst, klantinstructie of subverwerker.

11.1.5 [All] The Internal Audit / Compliance Reviewer MOET bewijsmateriaal over beleidsbeoordeling en geselecteerd bewijsmateriaal voor PII-beveiligingsmaatregelen in REG12 verifiëren volgens het goedgekeurde auditplan.

12. Gerelateerde beleidslijnen

12.1 Dit beleid moet worden gelezen in samenhang met:

12.1.1 PII01 - Beleid voor het privacy-informatiemanagementsysteem;

12.1.2 PII02 - Beleid inzake privacyrollen, verantwoordelijkheden en verantwoordingsplicht;

12.1.3 PII03 - Beleid inzake PII-verwerkingsinventaris en rechtsgrondslag;

12.1.4 PII07 - Beleid inzake privacyrisicobeoordeling en DPIA;

12.1.5 PII08 - Beleid inzake privacy by design en by default;

12.1.6 PII09 - Beleid inzake verzameling, gebruik, verstrekking en delen van PII;

12.1.7 PII10 - Beleid inzake bewaring, verwijdering en afvoer van PII;

12.1.8 PII12 - Beleid inzake privacybeheer van verwerkers, subverwerkers en derden;

12.1.9 PII13 - Beleid inzake internationale doorgifte van PII;

12.1.10 PII15 - Beleid inzake PII-incidenten en inbreukbeheer;

12.1.11 PII16 - Beleid inzake privacytraining, bewustwording en competentie;

12.1.12 PII17 - Beleid inzake PIMS-gedocumenteerde informatie en bewijsbeheer;

12.1.13 PII18 - Beleid inzake PIMS-monitoring, audit en verbetering.

13. Referentienormen en -raamwerken

13.1 ISO/IEC 27701:2025 - Clause 6.1.3; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.7; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5; 5.1.4; 5.1.6; 6.1.2; 7.1.1; 7.1.2].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.5.5; 4.6.3; 4.6.4; 4.7.5; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 7.1.3; 7.1.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.2; 11.1.1; 11.1.5].

13.3 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 10.1.3].

13.4 ISO/IEC 27701:2025 - Annex A.3.22; Annex A.3.23. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5].

13.5 ISO/IEC 27701:2025 - Annex A.3.25; Annex A.3.26. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.6 ISO/IEC 27701:2025 - Annex A.3.28; Annex A.3.29. Addressed by clauses [4.1.1; 4.1.2; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 7.1.1; 7.1.2].

13.7 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.15; Annex A.3.16. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.6.2; 4.6.3; 4.6.4; 4.7.2; 4.7.3; 5.1.9; 6.1.6; 8.1.4; 10.1.1; 11.1.5].

13.8 GDPR - Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.5; 4.2.6; 4.2.7; 4.3.2; 4.4.4; 4.5.1; 4.5.2; 4.6.1; 4.6.6; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 4.8.5; 5.1.1; 5.1.7; 6.1.4; 7.1.4; 9.1.3; 10.1.4].

13.9 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.10 ISO/IEC 27002:2022 - Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.11 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.1; 4.5.1; 4.6.2; 4.6.6; 4.7.6; 5.1.2; 6.1.1; 8.1.4; 10.1.1; 11.1.1].

13.12 ISO/IEC 29151:2022 - Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.7.1; 4.7.2; 4.7.4; 4.8.1; 4.8.2; 6.1.6; 11.1.5].