					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: PII17					Dokumenttitel: **Policy för hantering av dokumenterad information och underlag inom PIMS**							
Version: 1.0		Ikraftträdandedatum: 01.01.2025			Dokumentägare:							
X	Policy		Standard		Rutin		Formulär		Register		Övrigt	

Revisionshistorik				
Revisionsnummer	**Revisionsdatum**	**Ändringar**	**Granskad av**	**Processägare**

Godkännanden			
Namn	**Titel**	**Datum**	**Underskrift**

Ansluten till standarder och regelverk

Standard / regelverk	Klausul / kontroll / artikel	Tillämplighet	Täckningstyp	Kommentar
ISO/IEC 27701:2025	Clause 6.1.3	Both	Supporting	Dokumenterad information för tillämpbarhetsförklaring
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	PIMS-dokumenterad information
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Styrning av operativt underlag
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Underlag för övervakning
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Revisionsbevis
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Underlag för ledningens genomgång
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Underlag för avvikelse och korrigerande åtgärder
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Behandlingsregister för personuppgiftsansvarig
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Underlag för personuppgiftsbiträdesavtal och instruktioner
ISO/IEC 27701:2025	Annex A.3.14	Both	Primary	Skydd av poster
GDPR	Article 5(2)	Controller	Supporting	Underlag för ansvarsskyldighet
GDPR	Article 24	Controller	Supporting	Åtgärder och underlag för personuppgiftsansvarig
GDPR	Article 28	Both	Supporting	Dokumentation för personuppgiftsbiträde
GDPR	Article 30	Both	Supporting	Behandlingsregister
GDPR	Article 32	Both	Supporting	Skydd av underlag
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Underlag för efterlevnad av integritetskrav
ISO/IEC 29151:2022	Clause 18.1.4	Both	Supporting	Skydd av poster
ISO/IEC 27001:2022	Clause 7.5	Both	Supporting	Styrning av dokumenterad information
ISO/IEC 27002:2022	Control 5.33	Both	Supporting	Skydd av poster

ISO/IEC 27002:2022	Control 5.34	Both	Supporting	Skydd av integritet och PII

1. Omfattning

1.1 Denna policy anger obligatoriska krav för att skapa, godkänna, versionshantera, skydda, bevara, hämta, översätta, dra tillbaka och styrka PIMS-dokumenterad information med underlag.

1.2 Denna policy gäller PIMS-policyer, register, dokumenterade godkännanden, underlagsposter, revisionsbevis, poster från ledningens genomgång, underlag för korrigerande åtgärder och styrda översättningar som används för att visa PIMS-överensstämmelse.

1.3 Denna policy gäller i sammanhang med personuppgiftsansvarig, gemensamt personuppgiftsansvarig, personuppgiftsbiträde och underbiträde.

1.4 Denna policy skapar inte ett separat dokumentstyrningsregister. Styrningsunderlag för dokumenterad information upprätthålls genom de kanoniska PIMS-underlagsobjekten REG01 till REG12, där REG03 och REG12 används för kontrolltillämplighet, revision, avvikelse, korrigerande åtgärder och förbättringsunderlag.

2. Syfte

2.1 Syftet med denna policy är att säkerställa att PIMS-dokumenterad information är korrekt, styrd, åtkomlig för behöriga användare, skyddad mot obehörig ändring eller obehörigt röjande, bevarad för revisionsbarhet och indragen när den är inaktuell.

2.2 Denna policy stödjer beredskap för certifiering genom att säkerställa att underlag som behövs för att visa PIMS-överensstämmelse kan lokaliseras, verifieras, hämtas och kopplas till tillämpliga policyer, kontroller, behandlingsaktiviteter, risker, revisioner och korrigerande åtgärder.

3. Mål

3.1 Målen med denna policy är att:

3.1.1 definiera krav för styrning av PIMS-dokumenterad information;

3.1.2 upprätthålla underlagets integritet i REG01 till REG12;

3.1.3 säkerställa att godkännande av policyer och underlag är spårbart;

3.1.4 säkerställa att versionshistorik och beslut om indragning dokumenteras;

3.1.5 koppla PIMS-underlag till tillämpbarhetsförklaringen och policymappningar;

3.1.6 styra åtkomst till PIMS-dokument och underlagsposter;

3.1.7 stödja flerspråkig versionshantering av policyer och underlag;

3.1.8 möjliggöra snabb hämtning av revisionsbevis;

3.1.9 förhindra onödig dokumentstyrningsbyråkrati;

3.1.10 bevara poster med beredskap för revision för certifiering, kundförsäkran och ständig förbättring.

4. Policyuttalanden

4.1 Styrning av PIMS-dokumenterad information

4.1.1 [All] Privacy Lead / PIMS Manager MUST upprätthålla ett index över PIMS-dokumenterad information i REG12 före första PIMS-publicering och därefter kvartalsvis.

4.1.2 [All] Process Owner / Business Owner MUST identifiera dokumenterad information som krävs för varje ägd PII-behandlingsaktivitet i REG02 innan behandlingsaktiviteten inleds och därefter årligen.

4.1.3 [All] Privacy Lead / PIMS Manager MUST koppla tillämpliga PIMS-policyer, kontroller och underlagsförpliktelser till REG03 före varje policyutgåva och inom 15 arbetsdagar efter varje väsentlig ändring av kontrolltillämplighet.

4.1.4 [All] Privacy Lead / PIMS Manager MUST tilldela en åtkomstnivå och en känslighetsklassificering för underlag till varje kategori av PIMS-dokumenterad information i REG12 innan kategorin används.

4.2 Skapande, godkännande, versionshantering och publicering

4.2.1 [All] Privacy Lead / PIMS Manager MUST tilldela dokumentidentifierare, ägare, versionsnummer, godkännandestatus, ikraftträdandedatum och granskningsdatum i REG12 innan PIMS-dokumenterad information publiceras.

4.2.2 [All] Top Management MUST godkänna centrala PIMS-policyer och väsentliga policyändringar i REG12 före publicering.

4.2.3 [All] Privacy Lead / PIMS Manager MUST godkänna PIMS-underlagsmallar eller inbäddade registeravsnitt i REG12 före operativ användning.

4.2.4 [All] Privacy Lead / PIMS Manager MUST registrera versionshistorik och ändringsmotivering i REG12 innan uppdaterad PIMS-dokumenterad information ges ut.

4.2.5 [All] Privacy Lead / PIMS Manager MUST registrera kommunikation av godkända ändringar i PIMS-dokumenterad information i REG11 inom 30 dagar efter publicering.

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Undantag

9.1.1 [All] Process Owner / Business Owner MUST begära undantag avseende dokumenterad information eller underlagsstyrning i REG12 innan avvikelse från denna policy sker.

9.1.2 [All] Privacy Lead / PIMS Manager MUST bedöma varje undantag avseende dokumenterad information eller underlagsstyrning i REG12 inom 10 arbetsdagar efter begäran.

9.1.3 [All] Data Protection Officer / Privacy Advisor MUST registrera rådgivning i REG12 före godkännande av varje undantag som omfattar utlämnande av PII-underlag, översättningsavvikelse, bevarandekonflikt eller begränsning av revisionsbevis.

9.1.4 [All] Top Management MUST godkänna undantag för dokumenterad information som överstiger 30 dagar eller påverkar certifiering, högriskbehandling eller extern försäkran i REG12 innan undantaget träder i kraft.

9.1.5 [All] Privacy Lead / PIMS Manager MUST ange ett utgångsdatum som inte överstiger 90 dagar i REG12 för varje godkänt undantag avseende dokumenterad information eller underlagsstyrning.

9.1.6 [All] Privacy Lead / PIMS Manager MUST stänga eller ompröva varje undantag avseende dokumenterad information eller underlagsstyrning i REG12 inom fem arbetsdagar efter utgångsdatum.

10. Tillämpning

10.1.1 [All] Privacy Lead / PIMS Manager MUST registrera saknad, felaktig, ostyrd, inaktuell eller oåtkomlig PIMS-dokumenterad information som en avvikelse i REG12 inom fem arbetsdagar efter identifiering.

10.1.2 [All] Privacy Lead / PIMS Manager MUST förhindra publicering av PIMS-dokumenterad information när erforderligt underlag för godkännande, version, ägare eller ikraftträdandedatum saknas i REG12.

10.1.3 [All] Process Owner / Business Owner MUST förhindra inlämning av behandlingsunderlag till revision när erforderligt underlag för ägare, datum, status eller godkännande saknas i REG02.

10.1.4 [All] System Owner / Application Owner MUST ta bort obehörig åtkomst till lagringsplatser med PIMS-dokumenterad information och registrera borttagandet i REG12 inom en arbetsdag efter identifiering.

10.1.5 [All] Internal Audit / Compliance Reviewer MUST verifiera effektiviteten i korrigerande åtgärder för avvikelser avseende dokumenterad information i REG12 vid nästa planerade revision eller inom 60 dagar efter stängning, beroende på vilket som inträffar först.

11. Granskning och underhåll

11.1.1 [All] Privacy Lead / PIMS Manager MUST granska denna policy årligen och inom 30 dagar efter väsentlig ändring av krav på PIMS-dokumenterad information.

11.1.2 [All] Privacy Lead / PIMS Manager MUST granska denna policy inom 30 dagar efter en större revisionsiakttagelse, certifieringsavvikelse, ändring av lagringsplattform eller ändring av process för flerspråkig publicering.

11.1.3 [All] Data Protection Officer / Privacy Advisor MUST granska integritetsbetydande ändringar av denna policy i REG12 före godkännande.

11.1.4 [All] Top Management MUST godkänna väsentliga ändringar av denna policy i REG12 före publicering.

11.1.5 [All] Privacy Lead / PIMS Manager MUST registrera kommunikation av godkända ändringar av denna policy i REG11 inom 30 dagar efter publicering.

12. Relaterade policyer

12.1 Denna policy stöds av följande relaterade policyer:

12.1.1 PII01 - Policy för ledningssystem för hantering av integritetsinformation

12.1.2 PII02 - Policy för integritetsroller, ansvar och ansvarsskyldighet

12.1.3 PII03 - Policy för PII-behandlingsförteckning och rättslig grund

12.1.4 PII04 - Policy för integritetsmeddelande och transparens

12.1.5 PII05 - Policy för samtyckes- och preferenshantering

12.1.6 PII06 - Policy för hantering av registrerades rättigheter

12.1.7 PII07 - Policy för bedömning av integritetsrisker och DPIA

12.1.8 PII08 - Policy för integritetsskydd genom design och dataskydd som standard

12.1.9 PII09 - Policy för insamling, användning, utlämnande och delning av PII

12.1.10 PII10 - Policy för bevarande, radering och bortskaffning av PII

12.1.11 PII11 - Policy för korrekthet och kvalitet hos PII

12.1.12 PII12 - Policy för integritetshantering av personuppgiftsbiträden, underbiträden och tredje parter

12.1.13 PII13 - Policy för internationell överföring av PII

12.1.14 PII14 - Policy för PII-säkerhet och åtkomstkontroll

12.1.15 PII15 - Policy för hantering av PII-incidenter och personuppgiftsincidenter

12.1.16 PII16 - Policy för integritetsutbildning, medvetenhet och kompetens

12.1.17 PII18 - Policy för PIMS-övervakning, revision och förbättring

13. Referensstandarder och ramverk

13.1 Denna policy är mappad till följande standarder och regelverk. Mappningen förklarar hur policyn stödjer de angivna kraven och identifierar de interna klausuler som genomför eller stödjer dem.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.3** - Mappad till upprätthållande av PIMS-tillämpbarhetsförklaringen, poster om kontrolltillämplighet och koppling mellan policy och underlag. Addressed by clauses [4.1.3; 4.3.3; 6.1.3; 7.1.2].

13.2.2 **Clause 7.5** - Mappad till identifiering, godkännande, versionshantering, åtkomst, hämtning, bevarande, indragning, koppling av översättningsversioner och bevarandemetadata för dokumenterad information. 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** - Mappad till operativ planering och styrningsunderlag för behandlingsregister, underlagsmallar, kvalitet i operativt underlag och externt tillhandahållet underlag. Addressed by clauses [4.1.2; 4.2.3; 4.3.2; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1** - Mappad till upprätthållande av dokumenterat underlag för mätning, hämtningsprestanda, underlagsluckor, översättningsavvikelser och slutförd åtkomstgranskning för underlagsarkiv. 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** - Mappad till hämtning av revisionsbevis, revisionsurval, spårbarhet för revisionsbevis och revisionsiakttagelser som rör styrning av dokumenterad information. Addressed by clauses [4.3.4; 4.4.4; 6.1.3; 8.1.3; 10.1.5].

13.2.6 **Clause 9.3** - Mappad till underlag för ledningens genomgång, ledningens genomgång av styrning av dokumenterad information och granskning utförd av Top Management av prestation för underlagsstyrning. Addressed by clauses [6.1.2; 8.1.1; 8.1.2; 11.1.4].

13.2.7 **Clause 10.2** - Mappad till avvikelser i dokumenterad information, korrigerande åtgärder, undantagshantering, stängning och effektivitetsverifiering. 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** - Mappad till behandlingsregister för personuppgiftsansvarig, ansvarsskyldighetsposter, kvalitet i behandlingsunderlag och bevarande av underlag som stödjer skyldigheter för personuppgiftsansvarig. Addressed by clauses [4.1.2; 4.3.2; 4.5.1; 7.1.3].

13.2.9 **Annex A.2.2.2** - Mappad till personuppgiftsbiträdesavtal, kundinstruktioner, externt tillhandahållet underlag och underlagsstyrning för relationer med personuppgiftsbiträden. Addressed by clauses [5.1.7; 7.1.4].

13.2.10 **Annex A.3.14** - Mappad till skydd av PIMS-poster mot förlust, obehörig ändring, obehörig åtkomst, obehörigt utlämnande och otillbörlig bortskaffning. 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)** - Mappad till underlag för ansvarsskyldighet, spårbarhet för underlag, hämtning av underlag, avvikelseposter och poster med beredskap för revision som visar efterlevnad. 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** - Mappad till styrningsunderlag för personuppgiftsansvarig, godkännandeposter, policystyrning, ansvarsskyldighetsåtgärder, dokumenterad granskning och tillsyn från 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** - Mappad till dokumentation för personuppgiftsbiträden och underbiträden, kundinstruktionsunderlag, externt tillhandahållet processunderlag och styrning av utlämnande av underlag. Addressed by clauses [4.4.5; 5.1.7; 7.1.4].

13.3.4 **Article 30** - Mappad till underlag för behandlingsregister, kvalitetskrav för underlag, referenser till behandlingsaktiviteter och metadata om ägare/status för behandlingsunderlag. Addressed by clauses [4.1.2; 4.3.2; 7.1.3; 10.1.3].

13.3.5 **Article 32** - Mappad till skydd av underlagsarkiv, åtkomstbegränsningar, åtkomstgodkännanden, granskning av skydd för arkiv och borttagande av obehörig åtkomst. 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** - Mappad till underlag för efterlevnad av integritetskrav, hämtning av revisionsbevis, spårbarhet för underlag, stöd för oberoende granskning och underlag för korrigerande åtgärder. 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** - Mappad till skydd av PII-relaterade poster, bevarande av poster samt kontroller för åtkomst och radering av underlagsarkiv. 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** - Mappad till identifiering, godkännande, tillgänglighet, skydd, versionshantering, bevarande, disposition och styrning av externt krävd dokumenterad information. 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 - Mappad till skydd av PIMS-poster mot förlust, förstöring, förfalskning, obehörig åtkomst, obehörigt utlämnande och otillbörlig bortskaffning. 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 - Mappad till skydd av integritet och PII i dokumenterad information, underlagsarkiv, utlämnanden och åtkomststyrda poster. Addressed by clauses [4.1.4; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 6.1.5].