					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: PII01					Dokumenttitel: **Policy för ledningssystem för hantering av integritetsinformation**							
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 / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 4.1	Both	Primary	Kontext och fastställande av PIMS-roll
ISO/IEC 27701:2025	Clause 4.2	Both	Primary	Intressenter och krav
ISO/IEC 27701:2025	Clause 4.3	Both	Primary	PIMS-omfattning
ISO/IEC 27701:2025	Clause 4.4	Both	Primary	Inrättande och förbättring av PIMS
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Ledarskap och åtagande
ISO/IEC 27701:2025	Clause 5.2	Both	Primary	Integritetspolicy
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Roller och befogenheter
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	Risker och möjligheter
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Bedömning av integritetsrisk
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Riskbehandling av integritetsrisker och SoA
ISO/IEC 27701:2025	Clause 6.2	Both	Primary	Integritetsmål
ISO/IEC 27701:2025	Clause 6.3	Both	Primary	Planerade PIMS-ändringar
ISO/IEC 27701:2025	Clause 7.1	Both	Primary	Resurser
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Kompetens
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Medvetenhet
ISO/IEC 27701:2025	Clause 7.4	Both	Primary	Kommunikation
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumenterad information
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Operativ planering och styrning

ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Operativ bedömning av integritetsrisk
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Operativ riskbehandling av integritetsrisker
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Övervakning och utvärdering
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Internrevision
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Ledningens genomgång
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Ständig förbättring
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Avvikelse och korrigerande åtgärder
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9	Controller	Primary	Styrningsposter för personuppgiftsansvarig
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3	Processor	Primary	Avtal och ändamål för personuppgiftsbiträde
ISO/IEC 27701:2025	Annex A.3.3	Both	Primary	Koppling till policy för PII-säkerhet
GDPR	Article 5(2)	Controller	Supporting	Underlag för ansvarsskyldighet
GDPR	Article 24	Controller	Supporting	Åtgärder och policy för personuppgiftsansvarig
GDPR	Article 26	Joint Controller	Supporting	Arrangemang för gemensamt personuppgiftsansvar
GDPR	Article 28	Both	Supporting	Styrning av personuppgiftsbiträden
GDPR	Article 30	Both	Supporting	Register över behandling
GDPR	Article 32	Both	Supporting	Säkerhet i behandlingen
GDPR	Article 35	Controller	Supporting	DPIA-styrning
ISO/IEC 29100:2020	Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12	Both	Supporting	Dataskyddskontroller och principer

ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	PIA-process och förberedelse
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2; Annex A.2	Controller	Supporting	Program och policy för skydd av PII
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1	Both	Supporting	Integrering av organisatorisk integritetsrisk

1. Omfattning

1.1 Denna policy inrättar organisationens ledningssystem för hantering av integritetsinformation för behandling av PII i sammanhang där organisationen agerar som personuppgiftsansvarig, gemensamt personuppgiftsansvarig, personuppgiftsbiträde och underbiträde.

1.2 Denna policy gäller för:

1.2.1 PIMS-omfattning, kontext, intressenter och organisatoriska gränser;

1.2.2 fastställande av PIMS-roll för PII-behandlingsaktiviteter;

1.2.3 integritetspolicy, integritetsmål, bedömning av integritetsrisk, riskbehandling av integritetsrisker och PIMS-tillämpbarhetsförklaring;

1.2.4 PIMS-styrning, övervakning, internrevision, ledningens genomgång, avvikelse, korrigerande åtgärder och ständig förbättring;

1.2.5 dokumenterad information och underlag som behövs för att visa PIMS-överensstämmelse och ansvarsskyldighet.

1.3 I denna policy avses med väsentlig ändring varje ändring som påverkar PIMS-omfattning, ändamål med PII-behandling, PII-kategorier, kategorier av PII-huvudpersoner, behandlingsplatser, rollfördelning som personuppgiftsansvarig eller personuppgiftsbiträde, systemarkitektur, leverantörs- eller underbiträdesarrangemang, profil för integritetsrisk, tillämpliga rättsliga eller avtalsmässiga skyldigheter eller certifieringsomfattning.

2. Syfte

2.1 Denna policy fastställer de obligatoriska styrningskraven för att inrätta, införa, underhålla, övervaka och kontinuerligt förbättra PIMS.

2.2 Syftet med denna policy är att säkerställa att organisationen kan visa ansvarsskyldig, riskbaserad och evidensdriven hantering av PII-behandling inom tillämpliga PIMS-roller.

3. Mål

3.1 Målen med denna policy är att:

3.1.1 definiera PIMS-omfattning, kontext, gränser och rolltillämplighet;

3.1.2 tilldela styrningsansvar för PIMS med hjälp av kanoniska PIMS-roller;

3.1.3 fastställa integritetsmål och mätbara förväntningar på PIMS-prestanda;

3.1.4 upprätthålla en PIMS-tillämpbarhetsförklaring för valda och uteslutna kontroller;

3.1.5 integrera bedömning av integritetsrisk, riskbehandling av integritetsrisker och DPIA-styrning i PIMS-driften;

3.1.6 säkerställa att skyldigheter för personuppgiftsansvarig, gemensamt personuppgiftsansvarig, personuppgiftsbiträde och underbiträde identifieras innan behandling påbörjas;

3.1.7 upprätthålla underlag med beredskap för revision för beredskap för certifiering och ständig förbättring;

3.1.8 undvika onödiga roller, register, formulär och dubblerade operativa kontroller.

4. Policyuttalanden

4.1 Inrättande, kontext och omfattning för PIMS

4.1.1 [Both] Top Management SKA godkänna PIMS-omfattningen i REG01 före det första införandet av PIMS och inom 30 dagar från varje väsentlig ändring.

4.1.2 [Both] Privacy Lead / PIMS Manager SKA dokumentera externa och interna integritetsrelaterade kontextfrågor i REG01 årligen och inom 30 dagar från varje väsentlig ändring.

4.1.3 [Both] Privacy Lead / PIMS Manager SKA dokumentera relevanta intressenter och deras PIMS-krav i REG01 årligen och inom 30 dagar från varje väsentlig ändring.

4.1.4 [Both] Privacy Lead / PIMS Manager SKA underhålla sammanfattningen av PIMS-processernas samverkan i REG01 före varje ledningens genomgång.

4.2 Fastställande av PIMS-roll

4.2.1 [Both] Process Owner / Business Owner SKA klassificera organisationens PIMS-roll för varje PII-behandlingsaktivitet i REG02 innan behandlingsaktiviteten påbörjas.

4.2.2 [Joint Controller] Vendor / Procurement Owner SKA dokumentera ansvarsfördelningen mellan gemensamt personuppgiftsansvariga i REG08 innan gemensam behandling påbörjas.

4.2.3 [Processor] Vendor / Procurement Owner SKA dokumentera kundens behandlingsinstruktioner för aktiviteter som personuppgiftsbiträde i REG08 före onboarding av tjänst.

4.2.4 [Subprocessor] Vendor / Procurement Owner SKA dokumentera instruktioner från uppströmskund och godkända arrangemang för underbiträden i REG08 innan underbiträdesbehandling påbörjas.

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

9. Undantag

9.1 Begäran om undantag och godkännande

9.1.1 [All] Process Owner / Business Owner SKA dokumentera varje begärt undantag från denna policy i REG12 innan avvikelsen sker.

9.1.2 [Both] Privacy Lead / PIMS Manager SKA bedöma integritetsrisken för varje begärt undantag i REG04 före godkännande.

9.1.3 [Both] Top Management SKA godkänna undantag som överstiger accepterade tröskelvärden för integritetsrisk i REG12 före genomförande.

9.1.4 [Both] Privacy Lead / PIMS Manager SKA granska aktiva PIMS-undantag i REG12 kvartalsvis fram till stängning.

9.2 Stängning av undantag

9.2.1 [All] Process Owner / Business Owner SKA dokumentera underlag för stängning av undantag i REG12 senast det godkända undantagets utgångsdatum.

9.2.2 [Both] Internal Audit / Compliance Reviewer SKA verifiera underlag för stängning av utgångna undantag i REG12 under nästa planerade internrevision.

10. Tillämpning

10.1 Hantering av avvikelser

10.1.1 [All] Privacy Lead / PIMS Manager SKA registrera misstänkta avvikelser från denna policy i REG12 inom fem arbetsdagar från identifiering.

10.1.2 [All] Process Owner / Business Owner SKA genomföra godkända korrigerande åtgärder i REG12 senast tilldelat förfallodatum efter godkännande av avvikelsen.

10.1.3 [All] Top Management SKA granska olösta större PIMS-avvikelser i REG12 vid varje ledningens genomgång.

10.1.4 [All] Internal Audit / Compliance Reviewer SKA verifiera effektiviteten hos korrigerande åtgärder i REG12 inom 30 dagar från rapporterad stängning.

10.2 Eskalering

10.2.1 [All] Privacy Lead / PIMS Manager SKA eskalera försenade större korrigerande åtgärder till Top Management i REG12 inom fem arbetsdagar efter förfallodatumet.

10.2.2 [All] Top Management SKA registrera beslut om försenade större korrigerande åtgärder i REG12 inom 15 arbetsdagar från eskalering.

11. Granskning och underhåll

11.1 Policygranskning

11.1.1 [All] Privacy Lead / PIMS Manager SKA granska denna policy i REG12 årligen och inom 30 dagar från varje väsentlig ändring avseende lagkrav, organisation, behandling, teknik eller certifieringsomfattning.

11.1.2 [All] Data Protection Officer / Privacy Advisor SKA lämna dokumenterad rådgivning i REG12 före policygodkännande när väsentliga integritetsskyldigheter ändras.

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

11.1.4 [All] Privacy Lead / PIMS Manager SKA uppdatera REG01 och REG03 inom 15 arbetsdagar efter godkända policyändringar som ändrar PIMS-omfattning eller kontrolltillämplighet.

11.1.5 [All] Privacy Lead / PIMS Manager SKA registrera kommunikation av godkända policyändringar i REG11 inom 30 dagar från publicering.

12. Relaterade policyer

12.1 Denna policy stöds av följande relaterade policyer:

12.2 PII02 - Policy för integritetsroller, ansvar och ansvarsskyldighet

12.3 PII03 - Policy för PII-behandlingsregister och rättslig grund

12.4 PII07 - Policy för bedömning av integritetsrisk och DPIA

12.5 PII08 - Policy för integritetsskydd genom design och som standard

12.6 PII12 - Policy för personuppgiftsbiträden, underbiträden och datadelning

12.7 PII14 - Policy för PII-säkerhet och åtkomstkontroll

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

12.9 PII16 - Policy för integritetsutbildning, medvetenhet och kompetens

12.10 PII17 - Policy för PIMS-dokumenterad information och hantering av underlag

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

13. Referensstandarder och ramverk

13.1 Denna policy är mappad mot 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 4.1** - Mappad till fastställande av organisatorisk kontext, integritetsrelaterade kontextfrågor och tillämplighet för roll som personuppgiftsansvarig eller personuppgiftsbiträde för PIMS-aktiviteter. Addressed by clauses [4.1.2; 4.2.1; 6.1.3].

13.2.2 **Clause 4.2** - Mappad till identifiering av intressenter, PII-huvudpersoner, kunder, tillsynsmyndigheter, personuppgiftsbiträden, underbiträden och deras relevanta PIMS-krav. Addressed by clauses [4.1.3; 7.2.1; 11.1.1].

13.2.3 **Clause 4.3** - Mappad till att definiera, godkänna, underhålla och ändra den dokumenterade PIMS-omfattningen. Addressed by clauses [4.1.1; 6.1.3; 11.1.4].

13.2.4 **Clause 4.4** - Mappad till att inrätta, införa, underhålla och förbättra PIMS-processer och deras samverkan. Addressed by clauses [4.1.4; 7.1.1; 7.2.1].

13.2.5 **Clause 5.1** - Mappad till godkännande från Top Management, resurser, styrningsgranskning och ledarskap över PIMS-effektivitet och förbättring. Addressed by clauses [4.3.1; 5.1.1; 6.1.1; 8.1.4; 10.1.3].

13.2.6 **Clause 5.2** - Mappad till att underhålla denna integritetspolicy som godkänd dokumenterad information och kommunicera policyändringar. Addressed by clauses [4.3.1; 11.1.1; 11.1.3; 11.1.5].

13.2.7 **Clause 5.3** - Mappad till att tilldela och kommunicera PIMS-roller, ansvar och befogenheter. Addressed by clauses [5.1.1; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.8 **Clause 6.1.1** - Mappad till planering av åtgärder för PIMS-risker och möjligheter med hjälp av kontext, intressentkrav, mål och förbättringsunderlag. Addressed by clauses [4.1.2; 4.1.3; 4.4.1; 6.1.1; 8.1.1].

13.2.9 **Clause 6.1.2** - Mappad till krav på bedömning av integritetsrisk före ny eller väsentligt ändrad behandling och till underhåll av underlag för integritetsrisk. Addressed by clauses [4.4.1; 5.1.3; 8.2.4; 9.1.2].

13.2.10 **Clause 6.1.3** - Mappad till riskbehandling av integritetsrisker, val av kontroller, koppling till informationssäkerhetsprogram och underhåll av tillämpbarhetsförklaringen. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.3; 7.1.4; 8.2.2].

13.2.11 **Clause 6.2** - Mappad till att fastställa, mäta, övervaka, kommunicera och uppdatera PIMS-mål. Addressed by clauses [4.3.1; 4.3.2; 8.1.2; 8.1.4].

13.2.12 **Clause 6.3** - Mappad till planerade PIMS-ändringar och styrning av ändringar som påverkar omfattning, roller, kontroller och dokumenterad information. Addressed by clauses [4.1.1; 6.1.3; 7.1.1; 11.1.4].

13.2.13 **Clause 7.1** - Mappad till att fastställa och tillhandahålla resurser för inrättande, drift, underhåll och förbättring av PIMS. Addressed by clauses [5.1.1; 6.1.1; 7.1.1].

13.2.14 **Clause 7.2** - Mappad till kompetensförväntningar och underlag som stödjer PIMS-ansvar och rollutförande. Addressed by clauses [5.1.3; 5.1.8; 11.1.5].

13.2.15 **Clause 7.3** - Mappad till medvetenhet om integritetspolicyn, bidrag till PIMS-effektivitet och konsekvenser av avvikelser. Addressed by clauses [11.1.5; 10.1.1; 10.2.1].

13.2.16 **Clause 7.4** - Mappad till intern och extern kommunikation som är relevant för PIMS-styrning, policyändringar och eskalering. Addressed by clauses [6.2.1; 10.2.1; 11.1.5].

13.2.17 **Clause 7.5** - Mappad till skapande, underhåll, styrning, beredskap och bevarande av dokumenterad information och underlag. Addressed by clauses [4.5.1; 4.5.3; 7.1.6; 11.1.4].

13.2.18 **Clause 8.1** - Mappad till planering, införande och styrning av PIMS operativa processer och externt tillhandahållna processer. Addressed by clauses [4.4.4; 7.1.3; 7.1.5; 7.2.1].

13.2.19 **Clause 8.2** - Mappad till att utföra bedömningar av integritetsrisk vid planerade intervall och när betydande ändringar föreslås eller inträffar. Addressed by clauses [4.4.1; 8.2.4; 9.1.2].

13.2.20 **Clause 8.3** - Mappad till att genomföra planer för riskbehandling av integritetsrisker och bevara underlag för behandlingsresultat. Addressed by clauses [4.4.3; 7.1.3; 8.2.2].

13.2.21 **Clause 9.1** - Mappad till övervakning, mätning, analys, utvärdering, mätetal och rapportering av PIMS-effektivitet. Addressed by clauses [8.1.1; 8.1.2; 8.1.4; 8.2.1; 8.2.2; 8.2.3; 8.2.4].

13.2.22 **Clause 9.2** - Mappad till planering av internrevision, stickprov av underlag, revisionsresultat och oberoende granskning. Addressed by clauses [5.1.9; 6.2.1; 8.1.3; 9.2.2].

13.2.23 **Clause 9.3** - Mappad till underlag för ledningens genomgång, prestandagranskning, resultat från ledningens genomgång och förbättringsbeslut. Addressed by clauses [6.1.1; 6.1.2; 8.1.4; 10.1.3].

13.2.24 **Clause 10.1** - Mappad till ständig förbättring genom ledningens genomgång, mätetal, uppföljning av korrigerande åtgärder och policyunderhåll. Addressed by clauses [6.1.1; 6.2.2; 10.1.4; 11.1.1].

13.2.25 **Clause 10.2** - Mappad till hantering av avvikelser, korrigerande åtgärder, eskalering, stängning och verifiering av effektivitet. Addressed by clauses [4.5.2; 6.2.2; 6.2.3; 10.1.1; 10.1.2; 10.1.4; 10.2.1; 10.2.2].

13.2.26 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9** - Mappad till register över behandlingsändamål på den personuppgiftsansvariges sida, koppling till rättslig grund, fastställande av behov av DPIA, ansvarsfördelning mellan gemensamt personuppgiftsansvariga och register över behandlingsunderlag. Addressed by clauses [4.2.1; 4.2.2; 4.4.2; 4.5.1; 7.1.2; 8.2.1].

13.2.27 **Annex A.2.2.2; Annex A.2.2.3** - Mappad till kundavtal för personuppgiftsbiträden, dokumenterade kundinstruktioner och ändamålsbegränsningar för personuppgiftsbiträden. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.2.28 **Annex A.3.3** - Mappad till koppling till policy för PII-säkerhet, ägarskap för kontrollbaslinje för PII-säkerhet och status för informationssäkerhetskontroller i PIMS-tillämpbarhetsförklaringen. Addressed by clauses [4.3.4; 5.1.4; 7.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Mappad till underlag för ansvarsskyldighet, policygodkännande, klassificering av behandlingsroll, kontrolltillämplighet, övervakning, revision och poster över korrigerande åtgärder. Addressed by clauses [4.3.1; 4.5.1; 4.5.2; 6.1.1; 8.1.3].

13.3.2 **Article 24** - Mappad till styrningsåtgärder för personuppgiftsansvarig, policygodkännande, PIMS-mål, granskning av effektivitet och dokumenterat underlag för den personuppgiftsansvariges ansvarsskyldighet. Addressed by clauses [4.3.1; 4.3.2; 6.1.1; 8.1.4; 11.1.1].

13.3.3 **Article 26** - Mappad till att fastställa och dokumentera ansvarsfördelning mellan gemensamt personuppgiftsansvariga innan gemensam behandling påbörjas. Addressed by clauses [4.2.2; 5.1.7; 7.1.5].

13.3.4 **Article 28** - Mappad till styrningsposter för personuppgiftsbiträden och underbiträden, kundens behandlingsinstruktioner och styrning av externt tillhandahållna processer. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.3.5 **Article 30** - Mappad till register över behandlingsaktiviteter, rollklassificering, ansvarsposter för behandling och underlag som bevaras för revisionsbarhet. Addressed by clauses [4.2.1; 5.1.5; 7.1.2; 8.2.1].

13.3.6 **Article 32** - Mappad till styrning av PII-säkerhetsbaslinje, ägarskap för säkerhetskontroller, status för säkerhetsgenomförande och bekräftelse av operativ styrning. Addressed by clauses [4.3.4; 4.4.4; 5.1.4; 7.1.4].

13.3.7 **Article 35** - Mappad till fastställande av behov av DPIA och bedömning av integritetsrisk innan högriskbehandling eller väsentligt ändrad behandling som personuppgiftsansvarig fortsätter. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12** - Mappad till identifiering av dataskyddskontroller, integritetsprinciper, informationssäkerhet, efterlevnad av integritetskrav, revision, underlag och riskbaserad integritetsstyrning. Addressed by clauses [4.3.3; 4.3.4; 4.4.1; 4.5.1; 8.1.3; 10.1.4].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Mappad till PIA-styrning, fastställande av DPIA-utlösare, PIA-förberedelse, kriterier för integritetsrisk och dokumenterat underlag för bedömning av integritetsrisk. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4; 9.1.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2; Annex A.2** - Mappad till krav på program för skydd av PII, identifiering av krav på skydd av PII, riskbaserat urval av integritetskontroller och policyinriktning för skydd av PII. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.4].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1** - Mappad till organisatoriska principer för integritetsrisk, ledningens åtagande, integrering av integritetsrisk i PIMS-styrning och förståelse av organisationens roll vid PII-behandling. Addressed by clauses [4.1.2; 4.2.1; 4.4.1; 4.4.3; 6.1.1].