					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: PII18					Dokumenttitel: **Policy för PIMS-övervakning, revision och förbättring**							
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 6.2	Both	Supporting	Mätning av integritetsmål
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumenterad information om övervakning, revision och förbättring
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Övervakning av operativ planering och styrning
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Övervakning, mätning, analys 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.1.2.9	Controller	Supporting	Personuppgiftsansvarigs behandlingsregister används för revision
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Underlag för personuppgiftsbiträdesavtal och samarbete vid revision
GDPR	Article 5(2)	Controller	Supporting	Underlag för ansvarsskyldighet
GDPR	Article 24	Controller	Supporting	Personuppgiftsansvarigs åtgärder och granskning av effektivitet
GDPR	Article 28	Both	Supporting	Styrning av revision av och samarbete med personuppgiftsbiträden
GDPR	Article 30	Both	Supporting	Behandlingsregister som används för revision
GDPR	Article 32	Both	Supporting	Testning och utvärdering av säkerhetsåtgärder
GDPR	Article 39	Conditional	Supporting	DPO:s övervakning och revisionsrådgivning där tillämpligt

ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Integritetsefterlevnad, revision och oberoende tillsyn
ISO/IEC 29151:2022	Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	Granskning av PII-skydd och kontroller av efterlevnad
ISO/IEC 27001:2022	Clause 9.1	Both	Supporting	Övervakning och utvärdering av informationssäkerhet
ISO/IEC 27001:2022	Clause 9.2	Both	Supporting	Stöd för internrevision av ISMS
ISO/IEC 27001:2022	Clause 9.3	Both	Supporting	Stöd för ledningens genomgång av ISMS
ISO/IEC 27001:2022	Clause 10.1	Both	Supporting	Stöd för ständig förbättring av ISMS
ISO/IEC 27001:2022	Clause 10.2	Both	Supporting	Stöd för avvikelsehantering och korrigerande åtgärder i ISMS
ISO/IEC 27002:2022	Control 5.35	Both	Supporting	Oberoende granskning av informationssäkerhet
ISO/IEC 27002:2022	Control 5.36	Both	Supporting	Efterlevnadsgranskning av policyer och standarder
ISO 19011:2018	Clause 4; Clause 5; Clause 6; Clause 7	Both	Supporting	Principer, program, genomförande och kompetens för revision av ledningssystem

1. Omfattning

1.1 Denna policy definierar organisationens krav för PIMS-övervakning, mätning, analys, utvärdering, internrevision, ledningens genomgång, avvikelsehantering, korrigerande åtgärder och ständig förbättring.

1.2 Denna policy gäller för:

1.2.1 alla PIMS-processer, kontroller, policyer, register, underlagsobjekt, system, leverantörer, personuppgiftsbiträden, underbiträden och upplägg för datadelning inom PIMS-omfattningen;

1.2.2 organisationens sammanhang som personuppgiftsansvarig, gemensamt personuppgiftsansvarig, personuppgiftsbiträde och underbiträde;

1.2.3 den samlade övervakningen av PIMS-prestanda, integritetsmål, genomförandestatus för kontroller, revisionsiakttagelser, avvikelser, korrigerande åtgärder, åtgärder från ledningens genomgång och förbättringsåtgärder;

1.2.4 underlag som bevaras i REG12 och stödjande källunderlag som bevaras i REG01 till REG11.

1.3 Denna policy ersätter inte operativa övervakningskrav som definieras i andra PIMS-policyer. Den fastställer den samlade cykeln för prestandautvärdering, revision, genomgång och förbättring av PIMS.

1.4 I denna policy avser en större PIMS-avvikelse ett fel som väsentligt påverkar PIMS-omfattning, integritetsmål, ansvarsskyldighet för behandling av PII, riskbehandling av integritetsrisker, registrerades rättigheter, säkerhet i behandlingen, styrning av personuppgiftsbiträden eller underbiträden, beredskap för personuppgiftsincidenter, integriteten i dokumenterade underlag, certifieringsomfattning eller upprepat fel avseende samma krav inom en 12-månadersperiod.

1.5 I denna policy avser en väsentlig ändring varje ändring som påverkar PIMS-omfattning, ändamål med behandling av PII, PII-kategorier, kategorier av registrerade, behandlingsplatser, rollfördelning mellan personuppgiftsansvarig och personuppgiftsbiträde, systemarkitektur, leverantörs- eller underbiträdesarrangemang, integritetsriskprofil, tillämpliga rättsliga eller avtalsmässiga skyldigheter, revisionsomfattning, övervakningsmetod eller certifieringsomfattning.

2. Syfte

2.1 Syftet med denna policy är att säkerställa att organisationen utvärderar PIMS-prestanda, verifierar PIMS-överensstämmelse, identifierar avvikelser, korrigerar kontrollsvagheter och kontinuerligt förbättrar PIMS med hjälp av objektiva underlag.

2.2 Denna policy gör det möjligt för organisationen att visa att aktiviteter för PIMS-övervakning, revision, ledningens genomgång och förbättring är planerade, oberoende där så krävs, underlagsbaserade, tidsenliga och spårbara till ansvariga roller och kanoniska underlagsobjekt.

3. Mål

3.1 Målen med denna policy är att:

3.1.1 definiera en samlad process för PIMS-övervakning och mätning;

3.1.2 säkerställa att integritetsmål och PIMS-kontrollers prestanda mäts med dokumenterade underlag;

3.1.3 fastställa ett riskbaserat internrevisionsprogram för PIMS;

3.1.4 bevara oberoende och objektivitet i PIMS-revisionsaktiviteter;

3.1.5 säkerställa att ledningens genomgång får fullständiga och aktuella indata om PIMS-prestanda;

3.1.6 säkerställa att avvikelser registreras, bedöms, korrigeras och verifieras;

3.1.7 säkerställa att korrigerande åtgärder följs upp till stängning och granskas avseende effektivitet;

3.1.8 identifiera återkommande svagheter och förbättringsmöjligheter;

3.1.9 stödja beredskap för certifiering och ansvarsfull hantering av underlag;

3.1.10 undvika duplicering av operativa mätetal som redan definieras i relaterade PIMS-policyer.

4. Policyuttalanden

4.1 Ramverk för PIMS-övervakning och mätning

4.1.1 [Both] Privacy Lead / PIMS Manager ska definiera det samlade PIMS-övervakningsprogrammet i REG12 före den inledande PIMS-driften och därefter årligen.

4.1.2 [Both] Privacy Lead / PIMS Manager ska definiera mätmetod, frekvens, underlagskälla, mål och ansvarig roll för varje PIMS-mätetal i REG12 innan mätcykeln börjar.

4.1.3 [Both] Process Owner / Business Owner ska lämna övervakningsindata för behandlingsaktiviteter avseende PII från REG02 till Privacy Lead / PIMS Manager kvartalsvis.

4.1.4 [Both] Information Security Lead ska lämna statusindata för PII-säkerhetskontroller från REG03 till Privacy Lead / PIMS Manager kvartalsvis.

4.1.5 [Both] Vendor / Procurement Owner ska lämna statusindata för personuppgiftsbiträden, underbiträden, tredjepartsdelning och leverantörssäkring från REG08 till Privacy Lead / PIMS Manager kvartalsvis.

4.1.6 [All] Incident Response Coordinator ska lämna trendindata om integritetsincidenter och personuppgiftsincidenter från REG10 till Privacy Lead / PIMS Manager månadsvis och inom 10 arbetsdagar efter stängning av en större incident.

4.1.7 [Both] Privacy Lead / PIMS Manager ska konsolidera PIMS-övervakningsresultat i REG12 kvartalsvis.

4.2 Internrevisionsprogram för PIMS

4.2.1 [All] Internal Audit / Compliance Reviewer ska årligen upprätta ett riskbaserat internrevisionsprogram för PIMS i REG12 före den första planerade PIMS-revisionscykeln.

4.2.2 [All] Internal Audit / Compliance Reviewer ska definiera mål, kriterier, omfattning, metod, urvalsgrund och rapporteringsfrist för varje PIMS-revision i REG12 innan revisionsarbete påbörjas.

4.2.3 [All] Internal Audit / Compliance Reviewer ska registrera kontroller av revisorns oberoende och intressekonflikter i REG12 före varje revisionsuppdrag.

4.2.4 [All] Privacy Lead / PIMS Manager ska göra begärd styrd PIMS-dokumenterad information och registerunderlag tillgängliga via REG12 inom 10 arbetsdagar från en godkänd revisionsbegäran.

4.2.5 [Both] Internal Audit / Compliance Reviewer ska vid varje PIMS-revision testa genomförandestatus för tillämpliga PIMS-kontroller mot REG03.

4.2.6 [Both] Internal Audit / Compliance Reviewer ska registrera det valda underlagsurvalet för behandling av PII i REG12 under varje PIMS-revision.

4.2.7 [All] Internal Audit / Compliance Reviewer ska registrera PIMS-revisionsresultat i REG12 inom 15 arbetsdagar efter slutförd revision.

4.2.8 [All] Privacy Lead / PIMS Manager ska tilldela ägare av korrigerande åtgärder för accepterade PIMS-revisionsiakttagelser i REG12 inom 10 arbetsdagar från acceptans av revisionsresultat.

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

9. Undantag

9.1 Undantag för övervakning, revision och förbättring

9.1.1 [All] Process Owner / Business Owner ska begära varje undantag från denna policy i REG12 innan avvikelsen sker.

9.1.2 [All] Privacy Lead / PIMS Manager ska bedöma påverkan på integritet, certifiering, revision och korrigerande åtgärder för varje begärt undantag i REG12 inom 10 arbetsdagar från begäran.

9.1.3 [All] Data Protection Officer / Privacy Advisor ska registrera rådgivning i REG12 före godkännande av varje undantag som påverkar rättsliga skyldigheter, registrerades rättigheter, DPIA-åtaganden, kundrevisionsskyldigheter eller högriskbehandling.

9.1.4 [All] Top Management ska godkänna undantag som påverkar slutförande av revisionsschema, ledningens genomgång, större avvikelser, certifieringsomfattning eller högriskbehandling i REG12 innan undantaget träder i kraft.

9.1.5 [All] Privacy Lead / PIMS Manager ska ange ett utgångsdatum som inte överstiger 90 dagar i REG12 för varje godkänt undantag avseende övervakning, revision eller förbättring.

9.1.6 [All] Privacy Lead / PIMS Manager ska stänga eller ompröva varje undantag avseende övervakning, revision eller förbättring i REG12 inom fem arbetsdagar från utgångsdatum.

10. Tillämpning

10.1 Tillämpning av krav på övervakning, revision och förbättring

10.1.1 [All] Privacy Lead / PIMS Manager ska registrera en missad övervakningscykel, missad PIMS-revision, försenad ledningsgenomgång, saknat revisionsunderlag, försenad korrigerande åtgärd eller försenad förbättringsåtgärd som en avvikelse i REG12 inom fem arbetsdagar från identifiering.

10.1.2 [All] Internal Audit / Compliance Reviewer ska registrera allvarlighetsgrad för revisionsiakttagelser i REG12 innan revisionsrapporten utfärdas.

10.1.3 [All] Top Management ska kräva korrigerande åtgärd för varje större PIMS-avvikelse i REG12 inom 10 arbetsdagar från eskalering.

10.1.4 [All] Process Owner / Business Owner ska förhindra produktionssättning eller inlämning av extern säkerhetsförsäkran för högriskbehandling när erforderligt underlag för korrigerande åtgärd saknas i REG12 före produktionssättning eller inlämning.

10.1.5 [All] Privacy Lead / PIMS Manager ska eskalera upprepade missade frister för övervakning eller korrigerande åtgärder till Top Management i REG12 inom fem arbetsdagar efter den andra förekomsten under en 12-månadersperiod.

10.1.6 [All] Internal Audit / Compliance Reviewer ska verifiera stängning av tillämpningsåtgärder i REG12 vid nästa schemalagda revision eller inom 60 dagar från rapporterad stängning, beroende på vilket som inträffar först.

11. Granskning och underhåll

11.1 Granskning och underhåll av policyn

11.1.1 [All] Privacy Lead / PIMS Manager ska granska denna policy i REG12 årligen och inom 30 dagar från en väsentlig ändring av krav på PIMS-övervakning, revision, ledningens genomgång, korrigerande åtgärder eller certifiering.

11.1.2 [All] Internal Audit / Compliance Reviewer ska årligen granska PIMS-revisionsprogrammets effektivitet i REG12 efter den sista schemalagda revisionen för PIMS-verksamhetsåret.

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

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

11.1.5 [All] Privacy Lead / PIMS Manager ska uppdatera REG01 och REG03 inom 15 arbetsdagar efter godkända ändringar av denna policy som ändrar PIMS-omfattning eller kontrolltillämplighet.

11.1.6 [All] Privacy Lead / PIMS Manager ska registrera kommunikation av godkända ändringar av denna policy i REG11 inom 30 dagar från publicering.

12. Relaterade policyer

12.1 Denna policy stöds av följande relaterade policyer:

12.2 PII01 - Policy för ledningssystem för hantering av integritetsinformation

12.3 PII02 - Policy för integritetsroller, ansvar och ansvarsskyldighet

12.4 PII03 - Policy för PII-behandlingsregister och rättslig grund

12.5 PII04 - Policy för integritetsmeddelande och transparens

12.6 PII05 - Policy för samtyckes- och preferenshantering

12.7 PII06 - Policy för hantering av registrerades rättigheter

12.8 PII07 - Policy för bedömning av integritetsrisker och DPIA

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

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

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

12.12 PII11 - Policy för korrekthet och kvalitet hos PII

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

12.14 PII13 - Policy för internationell överföring av PII

12.15 PII14 - Policy för PII-säkerhet och åtkomstkontroll

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

12.17 PII16 - Policy för integritetsutbildning, medvetenhet och kompetens

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

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 6.2** - Mappad till definition, mätning, rapportering och granskning av PIMS-mål och PIMS-prestandamätetal. Addressed by clauses [4.1.2; 4.3.4; 8.1.1].

13.2.2 **Clause 7.5** - Mappad till upprätthållande av dokumenterad information för övervakningsresultat, revisionsprogram, revisionsresultat, underlag för ledningens genomgång, avvikelser, korrigerande åtgärder och förbättringsåtgärder. Addressed by clauses [4.1.7; 4.2.4; 4.2.7; 4.3.1; 4.4.1; 7.1.8; 11.1.1].

13.2.3 **Clause 8.1** - Mappad till drift av den planerade cykeln för PIMS-övervakning, revision, korrigerande åtgärder och förbättring som en del av PIMS operativa styrning. Addressed by clauses [4.1.1; 4.2.1; 7.1.1; 7.1.6].

13.2.4 **Clause 9.1** - Mappad till definition av vad som övervakas och mäts, konsolidering av övervakningsresultat, utvärdering av PIMS-prestanda och upprätthållande av mätunderlag. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.1.7; 8.1.1; 8.1.2; 8.1.4; 8.1.7].

13.2.5 **Clause 9.2** - Mappad till upprätthållande av internrevisionsprogram, revisionsplanering, kontroller av revisorns oberoende, urval av underlag, revisionsresultat och uppföljning av revisionsiakttagelser. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 8.1.3; 10.1.2].

13.2.6 **Clause 9.3** - Mappad till planering av ledningens genomgång, granskning av PIMS-prestanda, granskning av trender i revisioner och korrigerande åtgärder, godkännande av utdata och resursbeslut. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 6.1.7].

13.2.7 **Clause 10.1** - Mappad till identifiering, godkännande, genomförande och uppföljning av möjligheter till ständig förbättring av PIMS lämplighet, tillräcklighet och effektivitet. Addressed by clauses [4.3.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 7.1.6].

13.2.8 **Clause 10.2** - Mappad till registrering av avvikelser, rotorsaksanalys, planering av korrigerande åtgärder, genomförande av korrigerande åtgärder, effektivitetsverifiering, eskalering och tillämpning. Addressed by clauses [4.2.8; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 10.1.1; 10.1.3; 10.1.6].

13.2.9 **Annex A.1.2.9** - Mappad till personuppgiftsansvarigas behandlingsregister som används som underlagskällor för övervakning, revisionsurval och mätetal för behandlingsregistrets aktualitet. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.2.10 **Annex A.2.2.2** - Mappad till underlag för personuppgiftsbiträdesavtal, kundrevisioner, svar på säkerhetsförsäkran och personuppgiftsbiträdets samarbete som följs upp genom processer för leverantörs- och kundsäkring. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3 GDPR

13.3.1 **Article 5(2)** - Mappad till underlag för ansvarsskyldighet avseende övervakning, revision, ledningens genomgång, korrigerande åtgärder och ständig förbättring. Addressed by clauses [4.1.7; 4.2.7; 4.3.2; 4.4.2; 4.5.1].

13.3.2 **Article 24** - Mappad till personuppgiftsansvarigs styrningsåtgärder, granskning av effektivitet, ledningens genomgång, korrigerande åtgärder och dokumenterade förbättringsunderlag. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.5.2; 10.1.3].

13.3.3 **Article 28** - Mappad till underlag för personuppgiftsbiträden, underbiträden, kundrevisioner, tredjepartssäkring och leverantörssamarbete. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3.4 **Article 30** - Mappad till behandlingsregister som används som underlag för övervakning, revisionsurval, fullständighet hos underlagsobjekt och behandlingsregistrets aktualitet. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.3.5 **Article 32** - Mappad till övervakning och utvärdering av status för PII-säkerhetskontroller, underlag för tekniska kontroller och säkerhetsrelaterade effektivitetsunderlag. Addressed by clauses [4.1.4; 4.2.5; 5.1.4; 7.1.4; 8.1.2].

13.3.6 **Article 39** - Mappad till integritetsrådgivning, övervakningsobservationer, revisionsstöd och granskning av trender i integritetsefterlevnad av Data Protection Officer / Privacy Advisor där tillämpligt. Addressed by clauses [5.1.3; 6.1.6; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Mappad till verifiering av integritetsefterlevnad, interna eller oberoende revisioner, interna kontroller, tillsynsmekanismer och underlag för bedömning av integritetsrisker. Addressed by clauses [4.2.1; 4.2.3; 4.2.7; 4.5.1; 6.1.6; 8.1.7].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.2.2; Clause 18.2.3; Clause 18.2.4** - Mappad till oberoende granskning av PII-relaterad informationssäkerhet, efterlevnad av policyer och standarder samt teknisk efterlevnadsgranskning för PII-skydd. Addressed by clauses [4.2.3; 4.2.5; 7.1.4; 8.1.2; 10.1.6].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 9.1** - Mappad till indata från övervakning och utvärdering av informationssäkerhet som stödjer mätning av PIMS-prestanda och status för PII-säkerhetskontroller. Addressed by clauses [4.1.4; 8.1.2].

13.6.2 **Clause 9.2** - Mappad till stöd från ISMS-internrevision för PIMS-revisionsplanering, revisionsunderlag, revisionsresultat och slutförande av revisionsprogram. Addressed by clauses [4.2.1; 4.2.2; 4.2.7; 8.1.3].

13.6.3 **Clause 9.3** - Mappad till indata och utdata från ledningens genomgång för integrerad tillsyn över PIMS-prestanda och informationssäkerhetsprestanda. Addressed by clauses [4.3.1; 4.3.2; 4.3.5; 4.3.6].

13.6.4 **Clause 10.1** - Mappad till ständig förbättring av PIMS och den stödjande kontrollmiljön för informationssäkerhet. Addressed by clauses [4.5.1; 4.5.2; 4.5.6].

13.6.5 **Clause 10.2** - Mappad till avvikelsehantering, planering av korrigerande åtgärder, genomförande av korrigerande åtgärder och effektivitetsverifiering. Addressed by clauses [4.4.2; 4.4.4; 4.4.6; 4.4.7; 10.1.1].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.35 - Mappad till oberoende granskning, kontroller av revisorns oberoende, testning av revisionsunderlag och oberoende verifiering av korrigerande åtgärders effektivitet. Addressed by clauses [4.2.3; 4.2.5; 4.4.7; 10.1.6].

13.7.2 Control 5.36 - Mappad till efterlevnadsgranskning av PIMS- och informationssäkerhetspolicyer, genomförandestatus för kontroller och underlag för överensstämmelse med standarder. Addressed by clauses [4.1.4; 4.2.5; 4.5.3; 8.1.2].

13.8 ISO 19011:2018

13.8.1 **Clause 4; Clause 5; Clause 6; Clause 7** - Mappad till revisionsprinciper, hantering av revisionsprogram, revisionsgenomförande, underlagsbaserad revisionsrapportering, revisionsuppföljning och kompetensförväntningar för PIMS-revisioner. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.6; 4.2.7; 4.4.7; 5.1.9; 11.1.2].