					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: PII16					Dokumenttitel: **Policy för integritetsutbildning, medvetenhet och kompetens**							
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 7.2; Clause 7.3	Both	Primary	Kompetens och medvetenhet
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Kommunikation och dokumenterat underlag
ISO/IEC 27701:2025	Clause 8.1; Clause 9.1; Clause 10.2	Both	Supporting	Operativ styrning, mätning och förbättring
ISO/IEC 27701:2025	Annex A.3.17	Both	Primary	Medvetenhet, utbildning och träning avseende behandling av PII
GDPR	Article 5(2); Article 24; Article 28; Article 32; Article 39	Both	Supporting	Ansvarsskyldighet, styrning av personuppgiftsbiträden, säkerhet och DPO-uppgifter
ISO/IEC 27001:2022	Clause 7.2; Clause 7.3; Annex A control 6.3	Both	Supporting	Kompetens, medvetenhet och utbildning
ISO/IEC 27002:2022	Control 6.3	Both	Supporting	Vägledning om medvetenhet, utbildning och träning
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Informationssäkerhet och efterlevnad inom integritetsskydd

1. Omfattning

1.1 Denna policy fastställer organisationens krav på integritetsutbildning, medvetenhet och kompetens inom ledningssystem för hantering av integritetsinformation.

1.2 Denna policy gäller för personal, uppdragstagare, tillfälligt anställda, relevanta tredje parter, personuppgiftsbiträden, underbiträden och andra intressenter vars arbete kan påverka behandling av PII, PIMS-prestanda, registrerades rättigheter, integritetsrisk, informationssäkerhet kopplad till PII, instruktioner till personuppgiftsbiträden, personuppgiftsincidenter, dokumenterad information eller underlag för regelefterlevnad.

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

1.4 Denna policy omfattar:

1.4.1 identifiering av målgrupper för integritetsutbildning;

1.4.2 introduktionsutbildning;

1.4.3 årlig repetitionsutbildning;

1.4.4 rollbaserad och händelsestyrd utbildning;

1.4.5 underlag för genomförd utbildning;

1.4.6 eskalering vid uteblivet slutförande;

1.4.7 granskning av utbildningens effektivitet;

1.4.8 underlag för utbildningssäkring av personuppgiftsbiträden, underbiträden och tredje parter.

1.5 Denna policy skapar inte en separat utbildningsmatris, utbildningspanel, HR-register, kompetensregister, disciplinärt register eller kundutbildningsregister. Utbildningstilldelningar, slutföranden, påminnelser, kompetensunderlag och medvetenhetsunderlag registreras i REG11, medan undantag, eskaleringar, avvikelser, korrigerande åtgärder och granskningsunderlag registreras i REG12. Underlag för utbildningssäkring av personuppgiftsbiträden, underbiträden och tredje parter registreras i REG08 där det är relevant.

1.6 Denna policy duplicerar inte:

1.6.1 tilldelning av rollansvar i PII02;

1.6.2 krav på behandlingsförteckning och rättslig grund i PII03;

1.6.3 metodik för integritetsrisk och DPIA i PII07;

1.6.4 grindar för integritetsskydd genom design i PII08;

1.6.5 styrning av personuppgiftsbiträdets livscykel i PII12;

1.6.6 drift av PII-säkerhet och åtkomstkontroll i PII14;

1.6.7 arbetsflöde för PII-incidenter och personuppgiftsincidenter i PII15;

1.6.8 styrning av dokumenterad information i PII17;

1.6.9 styrning av övervakning, internrevision och förbättring i PII18.

2. Syfte

2.1 Syftet med denna policy är att säkerställa att personer vars arbete påverkar behandling av PII förstår sitt integritetsansvar, genomför lämplig utbildning enligt en fastställd periodicitet, upprätthåller rollrelevant kompetens och skapar granskningsbart underlag för utbildning, medvetenhet och eskalering.

2.2 Denna policy stödjer ett konsekvent genomförande av PIMS genom att använda REG11 som primärt bevisobjekt för utbildning och medvetenhet samt REG08, REG10 och REG12 som stödjande bevisobjekt.

3. Mål

3.1 Målen med denna policy är att:

3.1.1 definiera målgrupper för integritetsutbildning;

3.1.2 definiera krav på introduktionsutbildning;

3.1.3 definiera krav på årlig repetitionsutbildning;

3.1.4 definiera krav på rollbaserad integritetsutbildning;

3.1.5 registrera underlag för slutförande i REG11;

3.1.6 eskalera uteblivet slutförande via REG12;

3.1.7 upprätthålla underlag för utbildningssäkring av personuppgiftsbiträden, underbiträden och tredje parter i REG08 där det är relevant;

3.1.8 granska utbildningens effektivitet utan att skapa överdrivna mätetal eller dubblettregister;

3.1.9 säkerställa att utbildningsinnehållet fortsatt är anpassat till aktuella PIMS-policyer och väsentliga integritetsförpliktelser.

4. Policyuttalanden

4.1 Målgrupp och tilldelning för utbildning

4.1.1 [All] Privacy Lead / PIMS Manager ska definiera målgruppskategorier för PIMS-utbildning i REG11 innan varje årlig utbildningscykel inleds.

4.1.2 [All] Process Owner / Business Owner ska identifiera personal vars arbetsuppgifter omfattar behandling av PII i REG11 före introduktion, rolltilldelning eller väsentlig ändring av arbetsuppgifter.

4.1.3 [Conditional] System Owner / Application Owner ska identifiera användare som behöver utbildning i integritetsskydd för PII-system, privilegierad åtkomst eller administration i REG11 innan åtkomst aktiveras eller ändras väsentligt.

4.1.4 [Joint Controller] Privacy Lead / PIMS Manager ska registrera ansvarsfördelning för utbildning vid gemensamt personuppgiftsansvar i REG11 eller REG08 innan gemensam behandling påbörjas eller ändras väsentligt.

4.1.5 [Conditional] Data Protection Officer / Privacy Advisor ska identifiera behov av fördjupad integritetsutbildning i REG11 innan utbildning tilldelas roller som hanterar högriskbehandling, särskilda kategorier av PII, registrerades rättigheter, DPIA:er, internationella överföringar eller bedömning av personuppgiftsincidenter.

4.1.6 [All] Privacy Lead / PIMS Manager ska registrera tilldelad utbildningsmålgrupp, utbildningstyp, obligatoriskt slutdatum och ansvarig för underlag i REG11 innan varje årlig utbildningscykel inleds.

4.2 Introduktion och årlig utbildningsperiodicitet

4.2.1 [All] Privacy Lead / PIMS Manager ska tilldela grundläggande utbildning i integritetsmedvetenhet i REG11 inom 10 arbetsdagar efter introduktion för personal med åtkomst till PII eller PIMS-ansvar.

4.2.2 [All] Process Owner / Business Owner ska säkerställa att tilldelad personal slutför integritetsutbildning vid introduktion i REG11 innan oövervakad åtkomst till PII godkänns eller inom 30 dagar efter introduktion, beroende på vilket som inträffar först.

4.2.3 [All] Privacy Lead / PIMS Manager ska tilldela årlig repetitionsutbildning i integritetsskydd i REG11 minst en gång var 12:e månad.

4.2.4 [All] Process Owner / Business Owner ska bekräfta status för årlig repetitionsutbildning för tilldelad personal i REG11 senast det publicerade årliga förfallodatumet.

4.2.5 [Conditional] Privacy Lead / PIMS Manager ska tilldela riktad repetitionsutbildning i REG11 inom 30 dagar efter en väsentlig ändring av integritetspolicy, väsentlig ändring av PIMS-

process, revisionsiakttagelse, återkommande utbildningsbrist eller relevant lärdom från PII-incident.

[... 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 ska registrera en begäran om undantag från integritetsutbildning i REG12 innan en obligatorisk tidsfrist för slutförande förlängs.

9.1.2 [All] Privacy Lead / PIMS Manager ska godkänna eller avslå begäranden om undantag från integritetsutbildning i REG12 innan undantaget blir aktivt.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor ska ge råd om utbildningsundantag i REG12 före godkännande när undantaget påverkar högriskbehandling, särskilda kategorier av PII, hantering av rättigheter, incidenthantering, internationella överföringar eller certifieringsunderlag.

9.1.4 [Conditional] Top Management ska godkänna undantag från integritetsutbildning i REG12 före aktivering när undantaget påverkar upprepat uteblivet slutförande, privilegierad åtkomst till PII, behandling av PII med hög påverkan eller regulatoriskt riktat underlag.

9.1.5 [All] Privacy Lead / PIMS Manager ska definiera undantagsägare, utgångsdatum, kompenserande åtgärd och granskningsdatum i REG12 innan något undantag från integritetsutbildning godkänns.

9.1.6 [All] Process Owner / Business Owner ska stänga eller förnya godkända undantag från integritetsutbildning i REG12 före undantagets utgångsdatum.

10. Efterlevnad och tillämpning

10.1.1 [All] Privacy Lead / PIMS Manager ska registrera en utbildningsavvikelse i REG12 inom fem arbetsdagar när underlag för obligatorisk integritetsutbildning saknas, är ofullständigt, är försenat eller inte kan spåras till REG11.

10.1.2 [All] Process Owner / Business Owner ska säkerställa att försenad obligatorisk integritetsutbildning slutförs eller eskaleras i REG11 eller REG12 inom 10 arbetsdagar efter att förseningsstatus har registrerats.

10.1.3 [Conditional] System Owner / Application Owner ska begränsa ny åtkomst till personuppgifter med hög påverkan i REG12 när obligatorisk introduktionsutbildning eller rollbaserad integritetsutbildning fortsatt är ofullständig efter eskalering.

10.1.4 [Processor] Vendor / Procurement Owner ska eskalera saknat utbildningssäkringsunderlag för personuppgiftsbiträden, underbiträden eller extern arbetskraft i REG08 och REG12 inom fem arbetsdagar efter identifiering.

10.1.5 [Conditional] Incident Response Coordinator ska länka utbildningsrelaterade tillämpningsåtgärder till REG10 inom en arbetsdag när utbildningsbristen bidrog till en misstänkt eller bekräftad PII-incident.

10.1.6 [All] Internal Audit / Compliance Reviewer ska verifiera stängningsunderlag för korrigerande utbildningsåtgärder 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 ska granska denna policy och utbildningsinnehåll minst årligen och registrera granskningsresultatet i REG11 eller REG12.

11.1.2 [All] Privacy Lead / PIMS Manager ska granska denna policy inom 30 dagar efter en väsentlig ändring av PIMS-omfattning, integritetslagstiftning, behandlingsaktiviteter, rollmodell, incidentlärdomar, revisionsiakttagelser eller resultat av utbildningens effektivitet.

11.1.3 [Conditional] Data Protection Officer / Privacy Advisor ska granska integritetsmässigt betydande policyändringar 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 utbildningsinnehåll och tilldelningsunderlag i REG11 inom 30 dagar efter en godkänd väsentlig policyändring.

12. Relaterade policyer

12.1 Denna policy bör läsas tillsammans med:

12.2 PII01 - Policy för ledningssystem för hantering av integritetsinformation;

12.3 PII02 - Policy för integritetsroller, ansvar och ansvarsskyldighet;

12.4 PII03 - Policy för behandlingsförteckning och rättslig grund för PII;

12.5 PII04 - Policy för integritetsmeddelande och transparens;

12.6 PII05 - Policy för hantering av samtycke och preferenser;

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

12.13 PII13 - Policy för internationell överföring av PII;

12.14 PII14 - Policy för PII-säkerhet och åtkomstkontroll;

12.15 PII15 - Policy för hantering av PII-incidenter och personuppgiftsincidenter;

12.16 PII17 - Policy för dokumenterad information och underlag inom PIMS;

12.17 PII18 - Policy för övervakning, revision och förbättring inom PIMS.

13. Referensstandarder och ramverk

13.1 ISO/IEC 27701:2025 - Clause 7.2; Clause 7.3; Clause 7.4. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 7.1.1; 7.1.2; 7.1.3; 11.1.1; 11.1.5].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.4; 4.6.5; 6.1.1; 6.1.2; 6.1.3; 6.1.5; 7.1.7; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 9.1.1; 9.1.2; 9.1.5; 10.1.1; 10.1.2; 10.1.6; 11.1.1; 11.1.2; 11.1.4].

13.3 ISO/IEC 27701:2025 - Annex A.3.17. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 11.1.5].

13.4 GDPR - Article 5(2); Article 24; Article 28; Article 32; Article 39. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.4.4; 4.5.3; 4.5.4; 4.5.5; 5.1.1; 5.1.3; 5.1.7; 6.1.2; 6.1.3; 6.1.4; 7.1.4; 7.1.5; 9.1.3; 9.1.4; 10.1.3; 10.1.4; 10.1.5; 11.1.3].

13.5 ISO/IEC 27001:2022 - Clause 7.2; Clause 7.3; Annex A control 6.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.3; 4.3.1; 4.3.5; 4.4.1; 4.4.3; 4.5.1; 4.5.2; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 6.1.1; 7.1.1; 7.1.2; 8.1.1; 8.1.2; 8.1.3; 11.1.1].

13.6 ISO/IEC 27002:2022 - Control 6.3. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 10.1.2].

13.7 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.5.5; 4.6.4; 4.6.5; 5.1.3; 6.1.2; 6.1.3; 6.1.5; 8.1.5; 9.1.3; 10.1.1; 10.1.6; 11.1.2].