					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: PII14					Dokumenttitel: **Policy för PII-säkerhet och åtkomstkontroll**							
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 6.1.3; Clause 8.1	Both	Primary	Planering och drift av säkerhetskontroller för PII
ISO/IEC 27701:2025	Clause 7.5; Clause 9.1; Clause 10.2	Both	Supporting	Bevismaterial, övervakning och korrigerande åtgärder
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9	Both	Primary	Identitet och åtkomsträttigheter för behandling av PII
ISO/IEC 27701:2025	Annex A.3.22; Annex A.3.23	Both	Primary	Slutpunktsskydd och säker autentisering
ISO/IEC 27701:2025	Annex A.3.25; Annex A.3.26	Both	Primary	Loggning och kryptografiskt skydd
ISO/IEC 27701:2025	Annex A.3.28; Annex A.3.29	Both	Supporting	Applikationssäkerhet och säker arkitektur
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.15; Annex A.3.16	Both	Supporting	Skydd och granskning av poster
GDPR	Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32	Both	Primary	Säkerhet, ansvarsskyldighet och kontroller för personuppgiftsbiträden
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	Integrering av ISMS-kontroller
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	Vägledning för genomförande av säkerhetskontroller
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Principer för informationssäkerhet och efterlevnad av dataskyddskrav
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;	Both	Supporting	Säkerhetskontroller för skydd av PII

	Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4			

1. Omfattning

1.1 Denna policy fastställer PII-specifika krav på säkerhet och åtkomstkontroll för system, applikationer, tjänster, enheter, molnmiljöer och operativa processer som lagrar, överför, behandlar, har åtkomst till, administrerar eller skyddar PII.

1.2 Denna policy gäller i sammanhang där organisationen är personuppgiftsansvarig, gemensamt personuppgiftsansvarig, personuppgiftsbiträde eller underbiträde och där organisationen fastställer, driver, stöder eller förlitar sig på säkerhetskontroller för behandling av PII.

1.3 Denna policy omfattar följande säkerhetskontrollområden för PII:

1.3.1 säkerhetsbaslinje för personuppgifter och integrering med befintliga informationssäkerhetspolicyer;

1.3.2 åtkomstkontroll;

1.3.3 autentisering;

1.3.4 privilegierad åtkomst;

1.3.5 kryptering och säker lagring;

1.3.6 loggning och övervakning;

1.3.7 säker konfiguration och hantering av sårbarheter;

1.3.8 åtkomstkontroller för slutpunkter och molntjänster;

1.3.9 koppling av bevismaterial genom REG02, REG08, REG10 och REG12.

1.4 Denna policy ersätter inte ett fullständigt ledningssystem för informationssäkerhet, en nätverkssäkerhetspolicy, policy för säker utveckling, policy för säkerhetskopiering, slutpunktspolicy, molnsäkerhetspolicy, kryptografisk standard, rutin för hantering av sårbarheter eller rutin för incidenthantering.

1.5 Där sådana policyer redan finns fastställer denna policy de PII-specifika kopplings- och beviskrav som behövs för PIMS-säkring.

1.6 Denna policy duplicerar inte:

1.6.1 inventering av PII-behandling och ägarskap för rättslig grund i PII03;

1.6.2 metodik för bedömning av integritetsrisker och DPIA i PII07;

1.6.3 grindar för integritetsskydd genom design i PII08;

1.6.4 regler för insamling, användning, utlämnande och delning i PII09;

1.6.5 genomförande av bevarande, radering och bortskaffning i PII10;

1.6.6 styrning av personuppgiftsbiträdens livscykel i PII12;

1.6.7 kontroller av mekanismer för internationell överföring i PII13;

1.6.8 arbetsflöde för incidenter och personuppgiftsincidenter i PII15;

1.6.9 styrning av dokumenterad information i PII17;

1.6.10 PIMS-styrning av övervakning, revision och förbättring i PII18.

1.7 För denna policy är operativa loggar, utdata från säkerhetsverktyg, exporter från åtkomstgranskningar, sårbarhetsrapporter och konfigurationsunderlag beviskällor som bifogas till, sammanfattas i eller refereras av de kanoniska bevisobjekten.

1.8 De är inte separata PIMS-register.

2. Syfte

2.1 Syftet med denna policy är att säkerställa att PII skyddas genom lämpliga, riskanpassade och verifierbara säkerhets- och åtkomstkontroller under hela behandlingen.

2.2 Denna policy gör det möjligt för organisationen att visa att säkerhetskontroller för PII planeras, införs, granskas, övervakas och förbättras genom REG02, REG08, REG10 och REG12 utan att skapa dubbla säkerhetsregister eller ersätta befintliga informationssäkerhetspolicyer.

3. Mål

3.1 Målen med denna policy är att:

3.1.1 fastställa en baslinje för åtkomstkontroll till PII för system och behandlingsaktiviteter;

3.1.2 säkerställa att autentiseringskontroller är lämpliga i förhållande till PII:s känslighet och åtkomstsammanhang;

3.1.3 fastställa granskningskrav för privilegierad och vanlig åtkomst till PII;

3.1.4 fastställa förväntningar på kryptering och säker lagring av PII i vila, under överföring och i relevanta moln- eller slutpunktssammanhang;

3.1.5 fastställa förväntningar på loggning och övervakning av åtkomst till, ändringar av och administration av PII;

3.1.6 fastställa krav på underlag för säker konfiguration och sårbarheter för system som behandlar PII;

3.1.7 fastställa förväntningar på åtkomst via slutpunkter och molntjänster utan att skapa en fullständig policy för slutpunktssäkerhet eller molnsäkerhet;

3.1.8 koppla misstänkta säkerhetsincidenter som rör PII till REG10 utan att duplicera incidentarbetsflödet;

3.1.9 integrera med befintliga informationssäkerhetspolicyer där sådana finns;

3.1.10 upprätthålla bevismaterial med beredskap för revision endast genom REG02, REG08, REG10 och REG12.

4. Policyuttalanden

4.1 Säkerhetsbaslinje för personuppgifter och ISMS-integrering

4.1.1 [Both] Information Security Lead ska fastställa säkerhetsbaslinjen för personuppgifter för varje system eller tjänst som behandlar PII i REG12 innan systemet eller tjänsten tas i produktion eller ändras väsentligt.

4.1.2 [Both] System Owner / Application Owner ska registrera platsen för bevismaterial avseende genomförda säkerhetskontroller för PII i REG12 innan en befintlig informationssäkerhetskontroll används för PIMS-säkring.

4.1.3 [Controller] Process Owner / Business Owner ska identifiera PII:s känslighet, behandlingssammanhang och åtkomstbehov i REG02 innan ny eller väsentligt ändrad åtkomst till PII begärs.

4.1.4 [Processor] Vendor / Procurement Owner ska registrera kundens säkerhetsinstruktioner, gränser för kundens ansvar och säkerhetsåtaganden för personuppgiftsbiträdet i REG08 innan personuppgiftsbiträdets åtkomst till kundens PII påbörjas eller ändras väsentligt.

4.1.5 [Both] Privacy Lead / PIMS Manager ska verifiera att säkerhetsunderlag för personuppgifter är kopplat till REG02, REG08, REG10 eller REG12 innan behandlingsaktiviteten godtas som möjlig att granska inom PIMS.

4.2 Baslinje för åtkomstkontroll

4.2.1 [Both] System Owner / Application Owner ska begränsa åtkomst till PII till godkända roller och behöriga användare som är registrerade eller spårbara i REG02 eller REG12 innan åtkomsten aktiveras.

4.2.2 [Both] Process Owner / Business Owner ska godkänna det verksamhetsmässiga ändamålet med åtkomst till PII i REG02 eller REG12 innan System Owner / Application Owner tilldelar åtkomst.

4.2.3 [Both] System Owner / Application Owner ska granska användaråtkomst till system som behandlar personuppgifter med hög påverkan eller känslig PII minst kvartalsvis och registrera granskningsresultatet i REG12.

4.2.4 [Both] System Owner / Application Owner ska granska användaråtkomst till andra system som behandlar PII minst årligen och registrera granskningsresultatet i REG12.

4.2.5 [Both] System Owner / Application Owner ska ta bort eller ändra åtkomst till PII i REG12 inom en arbetsdag efter rolländring, uppsägning, avtalsslut eller när åtkomst inte längre behövs.

4.2.6 [Processor] Vendor / Procurement Owner ska bekräfta i REG08 att personuppgiftsbiträdets åtkomst till kundens PII är begränsad till dokumenterade kundinstruktioner innan åtkomst aktiveras eller ändras.

4.2.7 [Subprocessor] Vendor / Procurement Owner ska bekräfta i REG08 att underbiträdets åtkomst till PII är begränsad till auktoriserade underbiträdesaktiviteter innan underbiträdets åtkomst aktiveras eller ändras.

[... 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 [Both] Information Security Lead ska registrera varje undantag från ett krav på PII-säkerhet eller åtkomstkontroll i REG12 innan undantaget aktiveras.

9.1.2 [Both] Data Protection Officer / Privacy Advisor ska ge råd om PII-säkerhetsundantag med högre risk i REG12 före godkännande.

9.1.3 [Both] Top Management ska godkänna PII-säkerhetsundantag i REG12 före aktivering när undantaget påverkar personuppgifter med hög påverkan, känslig PII, privilegierad åtkomst, kryptering, loggning eller olösta högrisksårbarheter.

9.1.4 [Both] Information Security Lead ska fastställa undantagets utgångstid, kompenserande kontroll och granskningsdatum i REG12 före godkännande av undantaget.

9.1.5 [Both] System Owner / Application Owner ska åtgärda, förnya eller stänga utgångna PII-säkerhetsundantag i REG12 inom fem arbetsdagar efter utgång.

9.1.6 [Processor] Vendor / Procurement Owner ska registrera säkerhetsundantag hos personuppgiftsbiträde eller underbiträde som påverkar kundens PII i REG08 och REG12 före godtagande.

10. Tillämpning

10.1.1 [Both] Privacy Lead / PIMS Manager ska registrera avvikelser för saknat eller ofullständigt säkerhetsunderlag för personuppgifter i REG12 inom fem arbetsdagar efter identifiering.

10.1.2 [Both] Information Security Lead ska tilldela ägarskap för åtgärdande av brister i säkerhetskontroller för PII i REG12 inom fem arbetsdagar efter validering.

10.1.3 [Both] System Owner / Application Owner ska inaktivera eller begränsa obehörig, överdriven eller obestyrkt åtkomst till PII inom en arbetsdag efter validering och registrera åtgärden i REG12.

10.1.4 [Conditional] Incident Response Coordinator ska koppla tillämpningsåtgärder till REG10 inom en arbetsdag när ärendet rör en misstänkt eller bekräftad PII-incident.

10.1.5 [Both] Top Management ska granska återkommande eller högriskrelaterade PII-säkerhetsavvikelser i REG12 före ledningens genomgång.

11. Granskning och underhåll

11.1.1 [All] Privacy Lead / PIMS Manager ska granska denna policy tillsammans med Information Security Lead minst årligen och registrera granskningsresultatet i REG12.

11.1.2 [Both] Information Security Lead ska granska säkerhetsbaslinjen för personuppgifter i REG12 inom 30 dagar efter en väsentlig teknisk förändring, hotförändring, revisionsiakttagelse, incident eller regulatorisk förändring som påverkar PII-säkerhet.

11.1.3 [Both] System Owner / Application Owner ska uppdatera PII-säkerhetsbevismaterial på systemnivå i REG12 inom 30 dagar efter väsentlig ändring av arkitektur, åtkomst, konfiguration, sårbarhet eller loggning.

11.1.4 [Processor] Vendor / Procurement Owner ska granska bevismaterial för säkerhetsansvar avseende personuppgiftsbiträdens och underbiträdens PII i REG08 inom 30 dagar efter väsentlig tjänsteförändring, ändring av kundinstruktion eller ändring av underbiträde.

11.1.5 [All] Internal Audit / Compliance Reviewer ska verifiera bevismaterial för policygranskning och utvalda säkerhetskontroller för PII i REG12 enligt den godkända revisionsplanen.

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 PII-behandlingsregister och rättslig grund;

12.5 PII07 - Policy för bedömning av integritetsrisker och DPIA;

12.6 PII08 - Policy för integritetsskydd genom design och som standard;

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

12.8 PII10 - Policy för bevarande, radering och bortskaffning av PII;

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

12.10 PII13 - Policy för internationell överföring av PII;

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

12.12 PII16 - Policy för integritetsutbildning, medvetenhet och kompetens;

12.13 PII17 - Policy för dokumenterad information och bevismaterial inom PIMS;

12.14 PII18 - Policy för PIMS-övervakning, revision och förbättring.

13. Referensstandarder och ramverk

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].