					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: PII14					Dokumenttitel: **Politik for PII-sikkerhed og adgangsstyring**							
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:							
X	Politik		Standard		Procedure		Formular		Register		Andet	

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

Tilpasset relevante standarder og regler

Standard / regulering	Klausul / kontrol / artikel	Anvendelighed	Dækningstype	Kommentar
ISO/IEC 27701:2025	Clause 6.1.3; Clause 8.1	Both	Primary	Planlægning og drift af sikkerhedskontroller for PII
ISO/IEC 27701:2025	Clause 7.5; Clause 9.1; Clause 10.2	Both	Supporting	Revisionsbevismateriale, overvågning og korrigerende handling
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9	Both	Primary	Identitet og adgangsrettigheder ved behandling af PII
ISO/IEC 27701:2025	Annex A.3.22; Annex A.3.23	Both	Primary	Endepunktsbeskyttelse og sikker autentifikation
ISO/IEC 27701:2025	Annex A.3.25; Annex A.3.26	Both	Primary	Logning og kryptografisk beskyttelse
ISO/IEC 27701:2025	Annex A.3.28; Annex A.3.29	Both	Supporting	Applikationssikkerhed og sikker arkitektur
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.15; Annex A.3.16	Both	Supporting	Beskyttelse og gennemgang af registreringer
GDPR	Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32	Both	Primary	Sikkerhed, ansvarlighed og databehandlerkontroller
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	Integration med 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	Vejledning i implementering af sikkerhedskontroller
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Principper for informationssikkerhed og efterlevelse af databeskyttelse
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	Sikkerhedskontroller til beskyttelse af PII

	Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4			

1. Omfang

1.1 Denne politik fastsætter PII-specifikke krav til sikkerhed og adgangsstyring for systemer, applikationer, tjenester, enheder, cloudmiljøer og driftsprocesser, som lagrer, transmitterer, behandler, tilgår, administrerer eller beskytter PII.

1.2 Denne politik gælder i sammenhænge med dataansvarlig, fælles dataansvarlig, databehandler og underdatabehandler, hvor organisationen fastlægger, driver, understøtter eller baserer sig på sikkerhedskontroller for behandling af PII.

1.3 Denne politik omfatter følgende domæner for sikkerhedskontroller for PII:

1.3.1 PII-sikkerhedsbaseline og integration med eksisterende informationssikkerhedspolitikker;

1.3.2 adgangsstyring;

1.3.3 autentifikation;

1.3.4 privilegeret adgang;

1.3.5 kryptering og sikker lagring;

1.3.6 logning og overvågning;

1.3.7 sikker konfiguration og sårbarhedsstyring;

1.3.8 kontroller for endpoint- og cloudadgang;

1.3.9 evidenskobling via REG02, REG08, REG10 og REG12.

1.4 Denne politik erstatter ikke et fuldt ledelsessystem for informationssikkerhed, en netværkssikkerhedspolitik, en politik for sikker udvikling, en backuppolitik, en endpointpolitik, en cloud-sikkerhedspolitik, en kryptografisk standard, en procedure for sårbarhedsstyring eller en procedure for håndtering af sikkerhedshændelser. Hvor sådanne politikker allerede findes, fastsætter denne politik den PII-specifikke kobling og de evidenskrav, der er nødvendige for PIMS-assurance.

1.5 Denne politik duplikerer ikke:

1.5.1 fortegnelse over behandlingsaktiviteter og ejerskab til behandlingsgrundlag i PII03;

1.5.2 metode for risikovurdering vedrørende databeskyttelse og DPIA i PII07;

1.5.3 kontrolporte for databeskyttelse gennem design i PII08;

1.5.4 regler for indsamling, brug, videregivelse og deling i PII09;

1.5.5 udførelse af opbevaring, sletning og bortskaffelse i PII10;

1.5.6 styring af databehandlerlivscyklus i PII12;

1.5.7 kontroller for overførselsgrundlag ved international overførsel i PII13;

1.5.8 arbejdsgang for hændelser og brud i PII15;

1.5.9 styring af dokumenterede oplysninger i PII17;

1.5.10 PIMS-styring af overvågning, revision og forbedring i PII18.

1.6 I denne politik er driftslogfiler, output fra sikkerhedsværktøjer, eksport fra gennemgang af adgangsrettigheder, sårbarhedsrapporter og konfigurationsevidens evidenskilder, som vedhæftes til, sammenfattes i eller henvises af de kanoniske evidensobjekter. De er ikke særskilte PIMS-registre.

2. Formål

2.1 Formålet med denne politik er at sikre, at PII beskyttes af passende, risikotilpassede og reviderbare sikkerheds- og adgangskontroller gennem hele behandlingen.

2.2 Denne politik gør det muligt for organisationen at dokumentere, at sikkerhedskontroller for PII planlægges, implementeres, gennemgås, overvåges og forbedres via REG02, REG08, REG10 og

REG12 uden at oprette duplikerende sikkerhedsregistre eller erstatte eksisterende informationssikkerhedspolitikker.

3. Mål

3.1 Målene med denne politik er at:

3.1.1 fastsætte en baseline for adgangsstyring for PII i systemer og behandlingsaktiviteter;

3.1.2 sikre, at autentifikationskontroller er passende i forhold til følsomheden og adgangskonteksten for PII;

3.1.3 fastsætte krav til gennemgang af privilegeret og almindelig adgang til PII;

3.1.4 fastsætte forventninger til kryptering og sikker lagring af PII i hvile, under overførsel og i relevante cloud- eller endpointkontekster;

3.1.5 fastsætte forventninger til logning og overvågning af adgang til, ændringer af og administration af PII;

3.1.6 fastsætte evidenskrav vedrørende sikker konfiguration og sårbarheder for systemer, der behandler PII;

3.1.7 fastsætte forventninger til endpoint- og cloudadgang uden at oprette en fuld politik for endpoint- eller cloudsikkerhed;

3.1.8 koble mistænkte sikkerhedshændelser vedrørende PII til REG10 uden at duplikere hændelsesarbejdsgangen;

3.1.9 integrere med eksisterende informationssikkerhedspolitikker, hvor disse findes;

3.1.10 vedligeholde revisionsklart revisionsbevismateriale ved kun at bruge REG02, REG08, REG10 og REG12.

4. Politikerklæringer

4.1 PII-sikkerhedsbaseline og ISMS-integration

4.1.1 [Both] Information Security Lead SKAL fastlægge PII-sikkerhedsbaselinen for hvert system eller hver tjeneste, der behandler PII, i REG12, før systemet eller tjenesten sættes i produktion eller ændres væsentligt.

4.1.2 [Both] System Owner / Application Owner SKAL registrere placeringen af evidens for implementerede PII-sikkerhedskontroller i REG12, før en eksisterende informationssikkerhedskontrol anvendes som assurance i PIMS.

4.1.3 [Controller] Process Owner / Business Owner SKAL identificere PII-følsomheden, behandlingskonteksten og adgangsbehovet i REG02, før der anmodes om ny eller væsentligt ændret adgang til PII.

4.1.4 [Processor] Vendor / Procurement Owner SKAL registrere kundens sikkerhedsinstrukser, grænser for kundens ansvar og databehandlerens sikkerhedsforpligtelser i REG08, før databehandlerens adgang til kundens PII påbegyndes eller ændres væsentligt.

4.1.5 [Both] Privacy Lead / PIMS Manager SKAL verificere, at evidens for PII-sikkerhed er koblet til REG02, REG08, REG10 eller REG12, før behandlingsaktiviteten accepteres som reviderbar i PIMS.

4.2 Baseline for adgangsstyring

4.2.1 [Both] System Owner / Application Owner SKAL begrænse adgang til PII til godkendte roller og autoriserede brugere, som er registreret eller sporbare i REG02 eller REG12, før adgang aktiveres.

4.2.2 [Both] Process Owner / Business Owner SKAL godkende forretningsformålet med adgang til PII i REG02 eller REG12, før System Owner / Application Owner tildeler adgang.

4.2.3 [Both] System Owner / Application Owner SKAL gennemgå brugeradgang til systemer, der behandler PII med højt konsekvensniveau eller følsom PII, mindst kvartalsvist og registrere resultatet af gennemgangen i REG12.

4.2.4 [Both] System Owner / Application Owner SKAL gennemgå brugeradgang til andre systemer, der behandler PII, mindst årligt og registrere resultatet af gennemgangen i REG12.

4.2.5 [Both] System Owner / Application Owner SKAL fjerne eller ændre adgang til PII i REG12 senest én arbejdsdag efter rolleændring, fratrædelse, kontraktophør eller når adgang ikke længere er nødvendig.

4.2.6 [Processor] Vendor / Procurement Owner SKAL bekræfte i REG08, at databehandlerens adgang til kundens PII er begrænset til dokumenterede instrukser fra kunden, før adgang aktiveres eller ændres.

4.2.7 [Subprocessor] Vendor / Procurement Owner SKAL bekræfte i REG08, at underdatabehandlerens adgang til PII er begrænset til autoriserede underdatabehandlingsaktiviteter, før underdatabehandleradgang aktiveres eller ændres.

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Undtagelser

9.1.1 [Both] Information Security Lead SKAL registrere hver undtagelse fra et krav om sikkerhed eller adgangsstyring vedrørende PII i REG12, før undtagelsen aktiveres.

9.1.2 [Both] Data Protection Officer / Privacy Advisor SKAL rådgive om sikkerhedsundtagelser vedrørende PII med højere risiko i REG12 før godkendelse.

9.1.3 [Both] Top Management SKAL godkende sikkerhedsundtagelser vedrørende PII i REG12 før aktivering, når undtagelsen påvirker PII med højt konsekvensniveau, følsom PII, privilegeret adgang, kryptering, logning eller uafklarede højrisikosårbarheder.

9.1.4 [Both] Information Security Lead SKAL fastlægge undtagelsens udløb, kompenserende kontrol og gennemgangsdato i REG12 før godkendelse af undtagelsen.

9.1.5 [Both] System Owner / Application Owner SKAL afhjælpe, forny eller lukke udløbne sikkerhedsundtagelser vedrørende PII i REG12 senest fem arbejdsdage efter udløb.

9.1.6 [Processor] Vendor / Procurement Owner SKAL registrere sikkerhedsundtagelser hos databehandler eller underdatabehandler, der påvirker kundens PII, i REG08 og REG12 før accept.

10. Håndhævelse

10.1.1 [Both] Privacy Lead / PIMS Manager SKAL registrere afvigelser for manglende eller ufuldstændig sikkerhedsevidens vedrørende PII i REG12 senest fem arbejdsdage efter identifikation.

10.1.2 [Both] Information Security Lead SKAL tildele ejerskab til afhjælpning af svigt i sikkerhedskontroller for PII i REG12 senest fem arbejdsdage efter validering.

10.1.3 [Both] System Owner / Application Owner SKAL deaktivere eller begrænse uautoriseret, for omfattende eller udokumenteret adgang til PII senest én arbejdsdag efter validering og registrere handlingen i REG12.

10.1.4 [Conditional] Incident Response Coordinator SKAL koble håndhævelsestiltag til REG10 senest én arbejdsdag efter, at håndhævelsessagen omfatter en mistænkt eller bekræftet PII-hændelse.

10.1.5 [Both] Top Management SKAL gennemgå gentagne afvigelser eller højrisikoafvigelser vedrørende PII-sikkerhed i REG12 før ledelsens gennemgang.

11. Gennemgang og vedligeholdelse

11.1.1 [All] Privacy Lead / PIMS Manager SKAL gennemgå denne politik med Information Security Lead mindst årligt og registrere resultatet af gennemgangen i REG12.

11.1.2 [Both] Information Security Lead SKAL gennemgå PII-sikkerhedsbaselinen i REG12 senest 30 dage efter en væsentlig teknologi-, trussels-, revisions-, hændelses- eller regulatorisk ændring, der påvirker PII-sikkerheden.

11.1.3 [Both] System Owner / Application Owner SKAL opdatere systemniveau-evidens for PII-sikkerhed i REG12 senest 30 dage efter væsentlig ændring af arkitektur, adgang, konfiguration, sårbarhed eller logning.

11.1.4 [Processor] Vendor / Procurement Owner SKAL gennemgå evidens for PII-sikkerhedsansvar hos databehandlere og underdatabehandlere i REG08 senest 30 dage efter væsentlig ændring af tjeneste, kundeinstruks eller underdatabehandler.

11.1.5 [All] Internal Audit / Compliance Reviewer SKAL verificere evidens for politikgennemgang og udvalgt evidens for PII-sikkerhedskontroller i REG12 i henhold til den godkendte revisionsplan.

12. Relaterede politikker

12.1 Denne politik bør læses sammen med:

12.1.1 PII01 - Politik for ledelsessystem for privatlivsinformation;

12.1.2 PII02 - Politik for privatlivsroller, ansvar og ansvarlighed;

12.1.3 PII03 - Politik for fortegnelse over behandling af PII og behandlingsgrundlag;

12.1.4 PII07 - Politik for risikovurdering vedrørende databeskyttelse og DPIA;

12.1.5 PII08 - Politik for databeskyttelse gennem design og standardindstillinger;

12.1.6 PII09 - Politik for indsamling, brug, videregivelse og deling af PII;

12.1.7 PII10 - Politik for opbevaring, sletning og bortskaffelse af PII;

12.1.8 PII12 - Politik for databehandlere, underdatabehandlere og tredjepartsstyring af databeskyttelse;

12.1.9 PII13 - Politik for international overførsel af PII;

12.1.10 PII15 - Politik for håndtering af PII-hændelser og brud;

12.1.11 PII16 - Politik for privatlivstræning, bevidstgørelse og kompetence;

12.1.12 PII17 - Politik for dokumenterede oplysninger og evidensstyring i PIMS;

12.1.13 PII18 - Politik for overvågning, revision og forbedring i PIMS.

13. Referencestandarder og rammeværker

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].