

				Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: PII17				Dokumenttitel: Politik for PIMS-dokumenteret information og styring af bevismateriale							
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

Juridisk meddelelse (ophavsret og brugsbegrænsninger)
(C) 2025 Clarysec LLC. All rights reserved.

Dette dokument er Clarysec LLC's intellektuelle ejendom. Ingen del af dette dokument må kopieres, genbruges, distribueres eller ændres til kommercielle eller implementeringsmæssige formål uden udtrykkelig skriftlig tilladelse.

Uautoriseret brug er strengt forbudt og kan medføre retslige skridt.

For licensiering kontakt: info@clarysec.com

Tilpasset relevante standarder og regler

Standard / regulering	Klausul / kontrol / artikel	Anvendelighed	Dækningstype	Kommentar
ISO/IEC 27701:2025	Clause 6.1.3	Both	Supporting	Dokumenteret information om anvendelseserklæring
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	PIMS-dokumenteret information
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Styring af operationelt bevismateriale
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Bevismateriale vedrørende overvågning
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Revisionsbevismateriale
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Bevismateriale fra ledelsens gennemgang
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Bevismateriale for afvigelser og korrigerende handlinger
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Fortegnelser over dataansvarliges behandling
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Bevismateriale for databehandleraftaler og instrukser
ISO/IEC 27701:2025	Annex A.3.14	Both	Primary	Beskyttelse af registreringer
GDPR	Article 5(2)	Controller	Supporting	Bevismateriale for ansvarlighed
GDPR	Article 24	Controller	Supporting	Dataansvarliges foranstaltninger og bevismateriale
GDPR	Article 28	Both	Supporting	Databehandlerdokumentation
GDPR	Article 30	Both	Supporting	Fortegnelser over behandlingsaktiviteter
GDPR	Article 32	Both	Supporting	Beskyttelse af bevismateriale
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Bevismateriale for overholdelse af databeskyttelseskrav
ISO/IEC 29151:2022	Clause 18.1.4	Both	Supporting	Beskyttelse af registreringer
ISO/IEC 27001:2022	Clause 7.5	Both	Supporting	Styring af dokumenteret information

ISO/IEC 27002:2022	Control 5.33	Both	Supporting	Beskyttelse af registreringer
ISO/IEC 27002:2022	Control 5.34	Both	Supporting	Beskyttelse af privatliv og PII

1. Omfang

- 1.1 Denne politik fastsætter obligatoriske krav til oprettelse, godkendelse, versionsstyring, beskyttelse, opbevaring, genfinding, oversættelse, tilbagetrækning og dokumentation af PIMS-dokumenteret information.
- 1.2 Denne politik gælder for PIMS-politikker, registre, dokumenterede godkendelser, bevisregistreringer, revisionsbevismateriale, registreringer fra ledelsens gennemgang, bevismateriale for korrigerende handlinger og kontrollerede oversættelser, der bruges til at dokumentere PIMS-overensstemmelse.
- 1.3 Denne politik gælder for kontekster med dataansvarlig, fælles dataansvarlig, databehandler og underdatabehandler.
- 1.4 Denne politik etablerer ikke et særskilt register for dokumentstyring. Bevismateriale for styring af dokumenteret information vedligeholdes gennem de kanoniske PIMS-bevisobjekter REG01 til REG12, hvor REG03 og REG12 anvendes til kontrolanvendelighed, revision, afvigelser, korrigerende handlinger og bevismateriale for forbedringer.

2. Formål

- 2.1 Formålet med denne politik er at sikre, at PIMS-dokumenteret information er nøjagtig, styret, tilgængelig for autoriserede brugere, beskyttet mod uautoriseret ændring eller videregivelse, opbevaret med henblik på revisionsbarhed og tilbagetrukket, når den er forældet.
- 2.2 Denne politik understøtter revisionsberedskab til certificering ved at sikre, at det bevismateriale, der er nødvendigt for at dokumentere PIMS-overensstemmelse, kan lokaliseres, verificeres, hentes og knyttes til relevante politikker, kontroller, behandlingsaktiviteter, risici, revisioner og korrigerende handlinger.

3. Mål

3.1 Målene med denne politik er at:

- 3.1.1 fastlægge krav til styring af PIMS-dokumenteret information;
- 3.1.2 opretholde bevismaterialets integritet på tværs af REG01 til REG12;
- 3.1.3 sikre, at godkendelse af politikker og bevismateriale er sporbar;
- 3.1.4 sikre, at versionshistorik og beslutninger om tilbagetrækning dokumenteres;
- 3.1.5 knytte PIMS-bevismateriale til anvendelseserklæringen og politikortlægninger;
- 3.1.6 styre adgang til PIMS-dokumenter og registreringer af bevismateriale;
- 3.1.7 understøtte versionsstyring af politikker og bevismateriale på flere sprog;
- 3.1.8 muliggøre rettidig genfinding af revisionsbevismateriale;
- 3.1.9 forhindre unødigt dokumentstyringsbureaukrati;
- 3.1.10 bevare revisionsklare registreringer med henblik på certificering, kundedokumentation og løbende forbedring.

4. Politikerkklæringer

4.1 Styring af PIMS-dokumenteret information

- 4.1.1 [All] Privacy Lead / PIMS Manager SKAL vedligeholde et indeks over PIMS-dokumenteret information i REG12 før første PIMS-offentliggørelse og derefter kvartalsvist.
- 4.1.2 [All] Process Owner / Business Owner SKAL identificere den dokumenterede information, der kræves for hver ejet PII-behandlingsaktivitet, i REG02 før behandlingsaktiviteten påbegyndes og derefter årligt.
- 4.1.3 [All] Privacy Lead / PIMS Manager SKAL knytte relevante PIMS-politikker, kontroller og bevisforpligtelser til REG03 før hver politikudgivelse og inden for 15 arbejdsdage efter enhver væsentlig ændring i kontrolanvendelighed.

- 4.1.4 [All] Privacy Lead / PIMS Manager SKAL tildele et adgangsniveau og en følsomhedsklassificering af bevismateriale til hver kategori af PIMS-dokumenteret information i REG12, før kategorien anvendes.

4.2 Oprettelse, godkendelse, versionsstyring og offentliggørelse

- 4.2.1 [All] Privacy Lead / PIMS Manager SKAL tildele en dokumentidentifikator, ejer, versionsnummer, godkendelsesstatus, ikrafttrædelsesdato og gennemgangsdato i REG12, før PIMS-dokumenteret information offentliggøres.
- 4.2.2 [All] Top Management SKAL godkende centrale PIMS-politikker og væsentlige politikændringer i REG12 før offentliggørelse.
- 4.2.3 [All] Privacy Lead / PIMS Manager SKAL godkende PIMS-skabeloner for bevismateriale eller indlejrede registerafsnit i REG12 før operationel brug.
- 4.2.4 [All] Privacy Lead / PIMS Manager SKAL registrere versionshistorik og begrundelse for ændringer i REG12, før opdateret PIMS-dokumenteret information frigives.
- 4.2.5 [All] Privacy Lead / PIMS Manager SKAL registrere kommunikation af godkendte ændringer i PIMS-dokumenteret information i REG11 inden for 30 dage efter offentliggørelse.

[... 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 [All] Process Owner / Business Owner SKAL anmode om undtagelser vedrørende dokumenteret information eller styring af bevismateriale i REG12, før der afviges fra denne politik.
- 9.1.2 [All] Privacy Lead / PIMS Manager SKAL vurdere hver undtagelse vedrørende dokumenteret information eller styring af bevismateriale i REG12 inden for 10 arbejdsdage efter anmodningen.
- 9.1.3 [All] Data Protection Officer / Privacy Advisor SKAL registrere rådgivning i REG12 før godkendelse af enhver undtagelse, der omfatter videregivelse af PII-bevismateriale, oversættelsesafvigelse, opbevaringskonflikt eller begrænsning af revisionsbevismateriale.
- 9.1.4 [All] Top Management SKAL godkende undtagelser vedrørende dokumenteret information, der overstiger 30 dage eller påvirker certificering, højrisikobehandling eller ekstern assurance, i REG12, før undtagelsen træder i kraft.
- 9.1.5 [All] Privacy Lead / PIMS Manager SKAL fastsætte en udløbsdato på højst 90 dage i REG12 for hver godkendt undtagelse vedrørende dokumenteret information eller styring af bevismateriale.
- 9.1.6 [All] Privacy Lead / PIMS Manager SKAL lukke eller revurdere hver undtagelse vedrørende dokumenteret information eller styring af bevismateriale i REG12 inden for fem arbejdsdage efter udløb.

10. Håndhævelse

- 10.1.1 [All] Privacy Lead / PIMS Manager SKAL registrere manglende, unøjagtig, ustyret, forældet eller ikke-genfindelig PIMS-dokumenteret information som en afvigelse i REG12 inden for fem arbejdsdage efter identifikation.
- 10.1.2 [All] Privacy Lead / PIMS Manager SKAL forhindre offentliggørelse af PIMS-dokumenteret information, når krævet bevismateriale for godkendelse, version, ejer eller ikrafttrædelsesdato mangler i REG12.
- 10.1.3 [All] Process Owner / Business Owner SKAL forhindre indsendelse til revision af behandlingsbevismateriale, hvor krævet bevismateriale for ejer, dato, status eller godkendelse mangler i REG02.

10.1.4 [All] System Owner / Application Owner SKAL fjerne uautoriseret adgang til repositories med PIMS-dokumenteret information og registrere fjernelsen i REG12 inden for én arbejdsdag efter identifikation.

10.1.5 [All] Internal Audit / Compliance Reviewer SKAL verificere effektiviteten af korrigerende handlinger for afvigelser vedrørende dokumenteret information i REG12 ved næste planlagte revision eller inden for 60 dage efter lukning, alt efter hvad der indtræffer først.

11. Gennemgang og vedligeholdelse

11.1.1 [All] Privacy Lead / PIMS Manager SKAL gennemgå denne politik årligt og inden for 30 dage efter væsentlige ændringer i krav til PIMS-dokumenteret information.

11.1.2 [All] Privacy Lead / PIMS Manager SKAL gennemgå denne politik inden for 30 dage efter en væsentlig revisionskonstatering, certificeringsafvigelse, ændring af repositoryplatform eller ændring af proces for flersproget offentliggørelse.

11.1.3 [All] Data Protection Officer / Privacy Advisor SKAL gennemgå ændringer i denne politik med væsentlig betydning for databeskyttelse i REG12 før godkendelse.

11.1.4 [All] Top Management SKAL godkende væsentlige ændringer i denne politik i REG12 før offentliggørelse.

11.1.5 [All] Privacy Lead / PIMS Manager SKAL registrere kommunikation af godkendte ændringer i denne politik i REG11 inden for 30 dage efter offentliggørelse.

12. Relaterede politikker

12.1 Denne politik understøttes af følgende relaterede politikker:

12.2 PII01 - Politik for ledelsessystem for privatlivsinformation

12.3 PII02 - Politik for roller, ansvar og ansvarlighed vedrørende databeskyttelse

12.4 PII03 - Politik for fortegnelse over PII-behandling og behandlingsgrundlag

12.5 PII04 - Politik for privatlivsmeddelelse og gennemsigtighed

12.6 PII05 - Politik for samtykke- og præferencestyring

12.7 PII06 - Politik for håndtering af registreredes rettigheder

12.8 PII07 - Politik for risikovurdering vedrørende databeskyttelse og DPIA

12.9 PII08 - Politik for databeskyttelse gennem design og standardindstillinger

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

12.11 PII10 - Politik for opbevaring, sletning og bortskaffelse af PII

12.12 PII11 - Politik for PII-nøjagtighed og -kvalitet

12.13 PII12 - Politik for privatlivsstyring af databehandlere, underdatabehandlere og tredjeparter

12.14 PII13 - Politik for international overførsel af personhenførbare oplysninger (PII)

12.15 PII14 - Politik for PII-sikkerhed og adgangsstyring

12.16 PII15 - Politik for PII-hændelser og brud på persondatasikkerheden

12.17 PII16 - Politik for træning, bevidstgørelse og kompetence vedrørende databeskyttelse

12.18 PII18 - Politik for PIMS-overvågning, revision og forbedring

13. Referencestandarder og rammeværker

13.1 Denne politik er kortlagt til følgende standarder og regler. Kortlægningen forklarer, hvordan politikken understøtter de citerede krav, og identificerer de interne klausuler, der implementerer eller understøtter dem.

13.2 **ISO/IEC 27701:2025**

- 13.2.1 **Clause 6.1.3** - Kortlagt til vedligeholdelse af PIMS-anvendelseserklæringen, registreringer af kontrolanvendelighed og kobling mellem politik og bevismateriale. Addressed by clauses [4.1.3; 4.3.3; 6.1.3; 7.1.2].
- 13.2.2 **Clause 7.5** - Kortlagt til identifikation af dokumenteret information, godkendelse, versionsstyring, adgang, genfinding, bevaring, tilbagetrækning, kobling af oversættelsesversioner og metadata for opbevaring. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.5; 4.4.1; 4.4.2; 4.4.4; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.1; 4.6.2; 4.6.3; 4.6.4].
- 13.2.3 **Clause 8.1** - Kortlagt til operationel planlægning og styring af bevismateriale for behandlingsregistreringer, skabeloner for bevismateriale, kvalitet af operationelt bevismateriale og eksternt leveret bevismateriale. Addressed by clauses [4.1.2; 4.2.3; 4.3.2; 7.1.3; 7.1.4].
- 13.2.4 **Clause 9.1** - Kortlagt til vedligeholdelse af dokumenteret bevismateriale for måling, genfindingsperformance, mangler i bevismateriale, oversættelsesuoverensstemmelser og gennemførelse af adgangsgennemgang for repositories. Addressed by clauses [8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6].
- 13.2.5 **Clause 9.2** - Kortlagt til genfinding af revisionsbevismateriale, revisionsstikprøver, sporbarhed af revisionsbevismateriale og revisionskonstateringer vedrørende styring af dokumenteret information. Addressed by clauses [4.3.4; 4.4.4; 6.1.3; 8.1.3; 10.1.5].
- 13.2.6 **Clause 9.3** - Kortlagt til bevismateriale fra ledelsens gennemgang, ledelsens gennemgangs behandling af styring af dokumenteret information og gennemgang foretaget af Top Management af performance for styring af bevismateriale. Addressed by clauses [6.1.2; 8.1.1; 8.1.2; 11.1.4].
- 13.2.7 **Clause 10.2** - Kortlagt til afvigelser vedrørende dokumenteret information, korrigerende handlinger, undtagelseshåndtering, lukning og verifikation af effektivitet. Addressed by clauses [4.3.4; 6.1.4; 9.1.1; 9.1.2; 9.1.4; 9.1.5; 9.1.6; 10.1.1; 10.1.5].
- 13.2.8 **Annex A.1.2.9** - Kortlagt til dataansvarliges behandlingsregistreringer, ansvarlighedsregistreringer, kvalitet af behandlingsbevismateriale og opbevaring af bevismateriale, der understøtter dataansvarliges forpligtelser. Addressed by clauses [4.1.2; 4.3.2; 4.5.1; 7.1.3].
- 13.2.9 **Annex A.2.2.2** - Kortlagt til databehandleraftale, kundens instruks, eksternt leveret bevismateriale og styring af bevismateriale for databehandlerforhold. Addressed by clauses [5.1.7; 7.1.4].
- 13.2.10 **Annex A.3.14** - Kortlagt til beskyttelse af PIMS-registreringer mod tab, uautoriseret ændring, uautoriseret adgang, uautoriseret frigivelse og utilbørlig bortskaffelse. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.2; 4.5.4; 4.5.5; 10.1.4].

13.3 **GDPR**

- 13.3.1 **Article 5(2)** - Kortlagt til bevismateriale for ansvarlighed, sporbarhed af bevismateriale, genfinding af bevismateriale, registreringer af afvigelser og revisionsklare registreringer, der dokumenterer overholdelse. Addressed by clauses [4.1.1; 4.3.2; 4.3.3; 4.4.4; 4.5.4; 6.1.3; 8.1.3; 10.1.1].
- 13.3.2 **Article 24** - Kortlagt til dataansvarliges governancebevismateriale, godkendelsesregistreringer, politikstyring, ansvarlighedsforanstaltninger, dokumenteret gennemgang og tilsyn udøvet af Top Management. Addressed by clauses [4.2.2; 4.3.3; 6.1.2; 9.1.4; 11.1.4].
- 13.3.3 **Article 28** - Kortlagt til dokumentation for databehandlere og underdatabehandlere, bevismateriale for kundens instruks, eksternt leveret procesbevismateriale og styring af videregivelse af bevismateriale. Addressed by clauses [4.4.5; 5.1.7; 7.1.4].

13.3.4 **Article 30** - Kortlagt til bevismateriale for behandlingsregistreringer, kvalitetskrav til bevismateriale, referencer til behandlingsaktiviteter og metadata om ejer/status for behandlingsbevismateriale. Addressed by clauses [4.1.2; 4.3.2; 7.1.3; 10.1.3].

13.3.5 **Article 32** - Kortlagt til beskyttelse af repositories med bevismateriale, adgangsbegrænsninger, adgangsgodkendelser, gennemgang af repositorybeskyttelse og fjernelse af uautoriseret adgang. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Kortlagt til bevismateriale for overholdelse af databeskyttelseskrav, genfindning af revisionsbevismateriale, sporbarhed af bevismateriale, understøttelse af uafhængig gennemgang og bevismateriale for korrigerende handlinger. Addressed by clauses [4.3.3; 4.4.4; 4.6.3; 6.1.3; 8.1.3; 10.1.5].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.1.4** - Kortlagt til beskyttelse af PII-relaterede registreringer, bevaring af registreringer samt kontroller for adgang til og sletning i repositories med bevismateriale. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.5.2; 4.5.5; 10.1.4].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 7.5** - Kortlagt til identifikation af dokumenteret information, godkendelse, tilgængelighed, beskyttelse, versionsstyring, opbevaring, disponering og styring af eksternt krævet dokumenteret information. Addressed by clauses [4.1.1; 4.2.1; 4.2.4; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.6.4].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.33 - Kortlagt til beskyttelse af PIMS-registreringer mod tab, destruktion, forfalskning, uautoriseret adgang, uautoriseret frigivelse og utilbørlig bortskaffelse. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.7.2 Control 5.34 - Kortlagt til beskyttelse af privatliv og PII i dokumenteret information, repositories med bevismateriale, videregivelser og adgangsstyrede registreringer. Addressed by clauses [4.1.4; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 6.1.5].