					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: PII24					Dokumenttitel: **Politik for databeskyttelse ved CCTV og fysisk overvågning**						
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 7.5; Clause 8.1	Both	Primary	Dokumenterede og operationelle kontroller
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Overvågning og korrigerende handling
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9	Controller	Primary	Formål, behandlingsgrundlag, risikoudløser og registreringer
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Fordeling ved databehandler og fælles dataansvarlig
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10	Controller	Supporting	Forpligtelser over for registrerede og anmodninger
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9	Controller	Primary	Indsamling, behandling, minimering, opbevaring og bortskaffelse
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Registreringer og anmodninger vedrørende videregivelse
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Databehandleraftaler, instrukser, bistand og registreringer
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Databehandlerrettigheder og bistand ved videregivelse
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Beskyttelse af registreringer og logning
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Principper og ansvarlighed
GDPR	Article 6	Controller	Primary	Behandlingsgrundlag
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Gennemsigtighed og privatlivsmeddelelser

GDPR	Article 15; Article 16; Article 17; Article 18; Article 21	Controller	Supporting	Rettighedsanmodninger
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Styring, databehandlere, registreringer, sikkerhed, DPIA og rådgivning
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Formål, indsamling, minimering, opbevaring og videregivelse
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Gennemsigtighed, deltagelse, ansvarlighed, sikkerhed og efterlevelse
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Databeskyttelsesrisiko og DPIA-udløsere
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Privatlivskontroller til beskyttelse af PII
ISO/IEC 29151:2022	Clause 9.2.3; Clause 9.4.2; Clause 11.1.3	Both	Supporting	Kontroller for adgang og fysisk adgang
ISO/IEC 27002:2022	Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15	Both	Supporting	PII, fysisk overvågning, adgangsbegrænsning og logning

1. Omfang

1.1 Denne politik gælder for CCTV, videoovervågning, overvågning af besøgende, logfiler fra fysisk adgangsstyring, overvågningsregistreringer udført af vagter, systemer til overvågning af lokaler samt relaterede fysiske overvågningsaktiviteter, der indsamler eller på anden måde behandler PII.

1.2 Denne politik gælder for organisationer, der handler som dataansvarlige for deres egne lokaler og fysiske overvågningsaktiviteter.

1.3 Den gælder også for støtteaktiviteter som databehandler eller underdatabehandler, hvor organisationen driver, hoster, gennemgår, lagrer, videregiver, sletter eller på anden måde behandler overvågningsoptagelser, besøgsdata eller fysiske adgangslogfiler på vegne af en kunde.

1.4 Denne politik dækker fastlæggelse af overvågningsformål, godkendelse, privatlivsmeddelelse og skiltning, adgangsbegrænsninger, videregivelse, opbevaring, sletning, outsourcing, eskalering af hændelser, routing af rettighedsanmodninger, gennemgang og styring af bevismateriale.

1.5 Denne politik giver ikke rådgivning om ansættelsesret, juridiske kommentarer vedrørende samarbejdsudvalg, retshåndhævelsesprocedurer eller et særskilt CCTV-register.

1.6 Overvågningsspecifikt bevismateriale vedligeholdes i de kanoniske PIMS-bevisobjekter, der er angivet i denne politik.

2. Formål

2.1 Formålet med denne politik er at fastlægge privatlivskontroller for CCTV og fysisk overvågning, så overvågningsaktiviteter har et klart formål, er gennemsigtige og proportionale, er underlagt adgangsstyring, opbevares i definerede perioder, kun videregives gennem godkendte kanaler og understøttes af revisionsbart PIMS-bevismateriale.

2.2 Denne politik understøtter ensartet håndtering af overvågningsoptagelser, besøgsregistreringer, fysiske adgangslogfiler og relateret PII fra overvågning uden at oprette yderligere registre, komitéer, dashboards eller ikke-kanoniske roller.

3. Mål

3.1 Målene med denne politik er at:

3.1.1 definere overvågningsformål og behandlingsomfang, før overvågning påbegyndes;

3.1.2 dokumentere CCTV, fysisk adgang, overvågning af besøgende og fysiske overvågningsaktiviteter i REG02;

3.1.3 identificere overvågningsaktiviteter, der kræver gennemgang af databeskyttelsesrisiko eller DPIA-screening i REG04;

3.1.4 opretholde bevismateriale for gennemsigtige privatlivsmeddelelser og skiltning i REG07;

3.1.5 begrænse adgang, visning, eksport, videregivelse og opbevaring af PII fra overvågning;

3.1.6 route anmodninger fra registrerede gennem REG06;

3.1.7 styre udliciterede overvågningsudbydere og bevismateriale for datadeling gennem REG08;

3.1.8 eskalere mistænkte PII-hændelser relateret til overvågning gennem REG10;

3.1.9 registrere gennemgange, undtagelser, afvigelser, korrigerende handlinger, revisionskonstateringer og forbedringer i REG12.

4. Politikkerklæringer

4.1 Fortegnelse over overvågning, formål og godkendelse

4.1.1 [Controller] Process Owner / Business Owner MUST registrere hver CCTV-aktivitet, overvågning af besøgende, log fra fysisk adgangsstyring eller fysisk overvågningsaktivitet i REG02, før aktiviteten påbegyndes.

4.1.2 [Controller] Privacy Lead / PIMS Manager MUST validere REG02-posten for formål, behandlingsgrundlag, overvåget lokation, PII-kategorier, kategorier af registrerede,

opbevaring, privatlivsmeddelelse, adgang og videregivelsesfelter, før en ny eller væsentligt ændret overvågningsaktivitet aktiveres.

4.1.3 [Controller] Process Owner / Business Owner MUST registrere godkendte overvågede zoner, udelukkede zoner og indsamlingsgrænser i REG02, før kameraer, sensorer, besøgslogfiler eller logning af adgangsstyring aktiveres.

4.1.4 [Conditional] Process Owner / Business Owner MUST indhente en beslutning om databeskyttelsesrisiko i REG04, før der aktiveres overvågning, som omfatter systematisk overvågning, lydoptagelse, biometrisk identifikation, analysebaseret detektion, følsomme lokationer, sårbare personer eller ikke-åbenlys overvågning.

4.1.5 [Joint Controller] Privacy Lead / PIMS Manager MUST registrere fordelingen af fælles overvågningsansvar i REG08, før delt overvågning med en udlejer, facilitetspartner, kunde eller anden fælles dataansvarlig påbegyndes.

4.1.6 [Processor] Privacy Lead / PIMS Manager MUST registrere kundens overvågningsinstrukser og tilladte behandlingsgrænser i REG08, før overvågningsoptagelser, besøgsregistreringer eller fysiske adgangslogfiler behandles på vegne af en kunde.

4.2 Privatlivsmeddelelse og gennemsigtighed

4.2.1 [Controller] Process Owner / Business Owner MUST sikre, at bevismateriale for skiltning om overvågning eller tilsvarende just-in-time-privatlivsmeddelelse registreres i REG07, før overvågede områder åbnes for registrerede.

4.2.2 [Controller] Privacy Lead / PIMS Manager MUST koble hver privatlivsmeddelelse om overvågning i REG07 til det tilsvarende behandlingsformål i REG02 før offentliggørelse eller væsentlig ændring.

4.2.3 [Processor] Privacy Lead / PIMS Manager MUST levere støtteoplysninger til privatlivsmeddelelser om overvågning i REG08, når organisationen driver overvågningstjenester efter kundens instrukser.

4.2.4 [Conditional] Process Owner / Business Owner MUST registrere alternative gennemsigtighedsforanstaltninger i REG07 og REG04, før ikke-åbenlys overvågning eller nødovervågning aktiveres.

[... 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 [All] Privacy Lead / PIMS Manager MUST registrere hver undtagelse fra denne politik i REG12, før undtagelsen anvendes.

9.2 [Conditional] Data Protection Officer / Privacy Advisor MUST dokumentere databeskyttelsesrådgivning i REG04 eller REG12 før godkendelse af undtagelser, der omfatter ikke-åbenlys overvågning, lydoptagelse, biometrisk identifikation, analysebaseret overvågning eller følsomme overvågningslokationer.

9.3 [All] Top Management MUST godkende undtagelser, der overstiger 90 dage, i REG12 før forlængelse ud over den oprindelige undtagelsesperiode.

9.4 [All] Privacy Lead / PIMS Manager MUST gennemgå åbne overvågningsundtagelser i REG12 mindst månedligt indtil lukning.

10. Håndhævelse

10.1 [All] Privacy Lead / PIMS Manager MUST registrere svigt i overvågningskontroller som afvigelser i REG12 inden for fem arbejdsdage efter bekræftelse.

10.2 [Both] Information Security Lead MUST suspendere uautoriseret adgang til overvågningssystemer inden for én arbejdsdag efter bekræftelse og registrere handlingen i REG10 eller REG12.

10.3 [All] Top Management MUST tildele ejerskab for korrigerende handlinger i REG12 inden for 10 arbejdsdage ved gentagne eller væsentlige politikovertrædelser.

10.4 [Conditional] Incident Response Coordinator MUST indlede arbejdsgangen for PII-hændelser i REG10 ved mistanke om uautoriseret videregivelse, tab eller kompromittering af PII fra overvågning.

11. Gennemgang og vedligeholdelse

11.1 [All] Privacy Lead / PIMS Manager MUST gennemgå denne politik og relateret overvågningsbevismateriale i REG12 mindst årligt.

11.2 [Controller] Process Owner / Business Owner MUST revalidere hvert aktivt overvågningsformål, hver privatlivsmeddelelse, hvert lokationsomfang og hver opbevaringspost i REG02 og REG07 mindst årligt.

11.3 [Both] System Owner / Application Owner MUST revalidere adgang, logning, sletning og eksportkontroller for overvågningssystemer i REG12 mindst årligt og efter væsentlig systemændring.

11.4 [Conditional] Vendor / Procurement Owner MUST revalidere bevismateriale for udliciterede overvågningsudbydere i REG08 mindst årligt og før kontraktfornyelse.

11.5 [All] Privacy Lead / PIMS Manager MUST opdatere relateret REG02-, REG04-, REG07-, REG08-, REG10- eller REG12-bevismateriale inden for 30 kalenderdage efter godkendte politikændringer.

12. Relaterede politikker

12.1 PII02 - Politik for privatlivsroller, ansvar og ansvarlighed

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

12.3 PII04 - Politik for privatlivsmeddelelse og gennemsigtighed

12.4 PII06 - Politik for håndtering af registreredes rettigheder

12.5 PII07 - Politik for risikovurdering vedrørende databeskyttelse og DPIA

12.6 PII08 - Politik for databeskyttelse gennem design og standardindstillinger

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

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

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

12.10 PII13 - Politik for international overførsel af PII

12.11 PII14 - Politik for PII-sikkerhed og adgangsstyring

12.12 PII15 - Politik for håndtering af PII-hændelser og brud på persondatasikkerheden

12.13 PII17 - Politik for dokumenterede oplysninger og styring af bevismateriale i PIMS

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

12.15 PII19 - Medarbejderprivatlivspolitik

12.16 PII21 - Politik for databeskyttelse ved AI og automatiseret beslutningstagning

12.17 PII23 - Politik for cloud-PII-databehandlere

13. Referencestandarder og rammeværker

13.1 Denne politik er kortlagt til følgende standarder og reguleringer. 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 7.5; Clause 8.1** - Kortlagt til dokumenteret overvågningsbevismateriale, operationel planlægning, aktiveringskontroller, formålsregistreringer, kobling til privatlivsmeddelelse, adgangskonfiguration, opbevaringskonfiguration og ændringsstyring for CCTV og fysiske overvågningsaktiviteter. Addressed by clauses [4.1.1; 4.1.2; 4.2.2; 4.3.1; 4.4.1; 6.2; 7.1; 11.5].

13.2.2 **Clause 9.1; Clause 10.2** - Kortlagt til måling af overvågningskontroller, udbydergennemgang, adgangsgennemgang, revisionskonstateringer, afvigelser, korrigerende handlinger, eskalering af forsinkede handlinger og forbedringsbevismateriale. Addressed by clauses [4.6.4; 6.4; 6.5; 6.6; 8.1; 8.7; 10.1; 11.1].

13.2.3 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9** - Kortlagt til den dataansvarliges definition af overvågningsformål, dokumentation af behandlingsgrundlag, beslutninger om udløsere for databeskyttelsesrisiko og registreringer af overvågningsrelaterede behandlingsaktiviteter i REG02 og REG04. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.4.1; 6.2; 7.1; 11.2].

13.2.4 **Annex A.1.2.7; Annex A.1.2.8** - Kortlagt til fordeling ved udliciterede overvågningsudbydere, fordeling af fælles overvågningsansvar og bevismateriale for databehandler eller fælles dataansvarlig i REG08. Addressed by clauses [4.1.5; 4.6.1; 4.6.2; 5.7; 6.2; 7.6].

13.2.5 **Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10** - Kortlagt til overvågningsrelaterede forpligtelser over for registrerede, routing af anmodninger, bevaring, der er nødvendig for at vurdere anmodninger, og styringsbevismateriale for støtte til rettigheder. Addressed by clauses [4.5.1; 4.5.2; 5.2; 7.2; 11.5].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9** - Kortlagt til begrænsning af overvågningsindsamling, behandlingsgrænser, minimering, opbevaringsperioder, sletning, overskrivning, opbevaringstilbageholdelser og kontrol med udtrukne kopier. Addressed by clauses [4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 7.3; 7.5; 8.4].

13.2.7 **Annex A.1.5.4; Annex A.1.5.5** - Kortlagt til registreringer af ekstern videregivelse, håndtering af videregivelsesanmodninger, minimering før videregivelse og hændelsesrelaterede videregivelser, der involverer PII fra overvågning. Addressed by clauses [4.3.4; 4.5.4; 7.8; 10.4].

13.2.8 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7** - Kortlagt til databehandlerens kundeinstrukser, tilladte behandlingsgrænser, støtte til privatlivsmeddelelser, instrukser om opbevaring og sletning, bistand ved rettigheder og databehandlerregistreringer for udliciterede overvågningstjenester. Addressed by clauses [4.1.6; 4.2.3; 4.4.5; 4.5.3; 4.6.3].

13.2.9 **Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Kortlagt til databehandlerens støtte til kundens forpligtelser, godkendelse af videregivelse, registreringer af videregivelse, underretning om videregivelsesanmodninger og håndtering af juridisk bindende videregivelse af PII fra overvågning. Addressed by clauses [4.3.5; 4.5.3; 4.6.2; 4.6.3].

13.2.10 **Annex A.3.14; Annex A.3.25** - Kortlagt til beskyttelse af overvågningsregistreringer, begrænset adgang, gennemgang af privilegeret adgang, logning af adgang, inddæmning af uautoriseret adgang og logningsbevismateriale for overvågningssystemer. Addressed by clauses [4.3.2; 4.3.3; 4.5.5; 5.4; 7.4; 10.2; 11.3].

13.3 GDPR

13.3.1 **Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)** - Kortlagt til lovlighed, rimelighed, gennemsigtighed, formålsbegrænsning, dataminimering,

opbevaringsbegrænsning og ansvarlighedsbevismateriale for overvågningsaktiviteter. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.1; 4.4.2; 4.4.3; 6.1; 8.1; 11.2].

13.3.2 Article 6 - Kortlagt til dokumentation af behandlingsgrundlag for CCTV, overvågning af besøgende, fysiske adgangslogfiler og andre fysiske overvågningsaktiviteter. Addressed by clauses [4.1.2; 4.1.4; 7.1].

13.3.3 **Article 12; Article 13; Article 14** - Kortlagt til gennemsigtige privatlivsmeddelelser om overvågning, bevismateriale for skiltning, kobling mellem privatlivsmeddelelse og behandlingsformål, støtteoplysninger fra databehandler til privatlivsmeddelelser og alternative gennemsigtighedsforanstaltninger. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 7.2; 8.2; 11.2].

13.3.4 **Article 15; Article 16; Article 17; Article 18; Article 21** - Kortlagt til indsigt, berigtigelse, sletning, begrænsning, indsigelse, routing af anmodninger, bevaring, der er nødvendig for at vurdere anmodninger, og overvågningsrelateret kundebistand. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 7.8; 11.5].

13.3.5 **Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39** - Kortlagt til den dataansvarliges styring, fordeling ved fælles dataansvar, databehandlerstyring, fortegnelser over behandlingsaktiviteter, sikkerhed for overvågningssystemer, gennemgang af databeskyttelsesrisiko, DPIA-udløsere og databeskyttelsesrådgivning. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 4.3.2; 4.3.3; 4.5.4; 4.6.1; 4.6.2; 4.6.4; 5.1; 5.3; 6.3; 8.5; 10.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Kortlagt til formålsspecifikation, indsamlingsbegrænsning, dataminimering, anvendelsesbegrænsning, opbevaringsbegrænsning og videregivelsesbegrænsning for PII fra overvågning. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.4; 4.4.1; 4.4.2; 4.4.4; 7.8].

13.4.2 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12** - Kortlagt til gennemsigtighed, individuel deltagelse, ansvarlighed, informationssikkerhed, efterlevelsesgennemgang, adgangsgennemgang, routing af rettigheder, eskalering af hændelser og bevismateriale for korrigerende handlinger. Addressed by clauses [4.2.1; 4.2.2; 4.3.2; 4.3.3; 4.5.1; 4.5.4; 6.1; 8.7; 10.1].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 5.1; Clause 6.2** - Kortlagt til screening for databeskyttelsesrisiko og DPIA-udløsere ved systematisk, ikke-åbenlys, lydbaseret, biometrisk, analyseaktiveret, følsom lokationsbaseret, sårbar personrelateret eller anden fysisk overvågning med højere risiko. Addressed by clauses [4.1.4; 4.2.4; 5.3; 6.3; 7.5; 9.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10** - Kortlagt til PII-beskyttelseskontroller for formål, indsamling, minimering, opbevaring, videregivelse og registreredes deltagelse i overvågningskontekster. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.4.1; 4.4.3; 4.5.1; 7.2; 8.2].

13.6.2 **Clause 9.2.3; Clause 9.4.2; Clause 11.1.3** - Kortlagt til adgangstildeling, begrænsning af informationsadgang og kontroller for fysisk adgang, der er relevante for adgang til overvågningssystemer og registreringer fra fysisk adgangsstyring. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.5.5; 5.4; 7.4; 10.2; 11.3].

13.7 ISO/IEC 27002:2022

13.7.1 Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15 - Kortlagt til privatliv og beskyttelse af PII, fysisk adgang, fysisk sikkerhedsovervågning, privilegeret adgang, begrænsning af

informationsadgang og logningskontroller for CCTV og fysiske overvågningssystemer. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.5.5; 5.4; 7.3; 7.4; 8.3; 10.2; 11.3].