					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: PII24					Dokumenttitel: **Integritetspolicy för CCTV och fysisk övervakning**							
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 7.5; Clause 8.1	Both	Primary	Dokumenterade och operativa kontroller
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Övervakning och korrigerande åtgärder
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	Ändamål, rättslig grund, riskutlösare och register
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Fördelning mellan personuppgiftsbiträde och gemensamt personuppgiftsansvariga
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	Skyldigheter och begäranden avseende registrerade
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	Insamling, behandling, minimering, bevarande och bortskaffning
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Register över utlämnanden och begäranden
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	Biträdesavtal, instruktioner, stöd och register
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	Biträdets stöd för rättigheter och utlämnanden
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Skydd av register och loggning
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Principer och ansvarsskyldighet
GDPR	Article 6	Controller	Primary	Rättslig grund
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Transparens och integritetsmeddelanden

GDPR	Article 15; Article 16; Article 17; Article 18; Article 21	Controller	Supporting	Rättighetsbegäranden
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Styrning, personuppgiftsbiträden, register, säkerhet, DPIA och rådgivning
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Ändamål, insamling, minimering, bevarande och utlämnande
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Transparens, deltagande, ansvarsskyldighet, säkerhet och efterlevnad
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Integritetsrisk och DPIA-utlösare
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Dataskyddskontroller för skydd av PII
ISO/IEC 29151:2022	Clause 9.2.3; Clause 9.4.2; Clause 11.1.3	Both	Supporting	Åtkomstkontroll och kontroller för fysiskt tillträde
ISO/IEC 27002:2022	Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15	Both	Supporting	PII, fysisk övervakning, åtkomstbegränsning och loggning

1. Omfattning

1.1 Denna policy gäller CCTV, videoövervakning, besöksövervakning, loggar över fysisk tillträdeskontroll, övervakningsuppgifter som hanteras av väktare, system för övervakning av lokaler samt relaterade fysiska övervakningsaktiviteter som samlar in eller på annat sätt behandlar PII.

1.2 Denna policy gäller organisationer som agerar som personuppgiftsansvariga för PII avseende egna lokaler och fysiska övervakningsaktiviteter.

1.3 Denna policy gäller även stödaktiviteter som personuppgiftsbiträde eller underbiträde där organisationen driver, tillhandahåller drift för, granskar, lagrar, lämnar ut, raderar eller på annat sätt behandlar övervakningsmaterial, besöksdata eller loggar över fysiskt tillträde på uppdrag av en kund.

1.4 Denna policy omfattar definition av övervakningsändamål, godkännande, information och skyltning, åtkomstbegränsningar, utlämnande, bevarande, radering, outsourcing, incidenteskalering, dirigering av rättighetsbegäranden, granskning och hantering av underlag.

1.5 Denna policy tillhandahåller inte arbetsrättslig rådgivning, rättsliga kommentarer om arbetstagarrepresentation, rutiner för brottsbekämpande myndigheter eller ett särskilt CCTV-register.

1.6 Övervakningsspecifikt underlag bevaras i de kanoniska PIMS-underlagsobjekt som anges i denna policy.

2. Syfte

2.1 Syftet med denna policy är att fastställa dataskyddskontroller för CCTV och fysisk övervakning så att övervakningsaktiviteter har ett tydligt ändamål, är transparenta och proportionerliga, omfattas av åtkomstkontroll, bevaras under definierade perioder, lämnas ut endast via godkända kanaler och stöds av PIMS-underlag som kan granskas.

2.2 Denna policy stödjer konsekvent hantering av övervakningsmaterial, besöksregister, loggar över fysiskt tillträde och relaterad övervaknings-PII utan att skapa ytterligare register, kommittéer, kontrollpaneler eller icke-kanoniska roller.

3. Mål

3.1 Målen med denna policy är att:

3.1.1 definiera övervakningsändamål och behandlingens omfattning innan övervakning inleds;

3.1.2 dokumentera CCTV, fysiskt tillträde, besöksövervakning och fysiska övervakningsaktiviteter i REG02;

3.1.3 identifiera övervakningsaktiviteter som kräver granskning av integritetsrisker eller DPIA-screening i REG04;

3.1.4 upprätthålla underlag för transparent information och skyltning i REG07;

3.1.5 begränsa åtkomst, visning, export, utlämnande och bevarande av övervaknings-PII;

3.1.6 dirigera registrerades begäranden via REG06;

3.1.7 hantera outsourcade övervakningsleverantörer och underlag för datadelning via REG08;

3.1.8 eskalera misstänkta övervakningsrelaterade PII-incidenter via REG10;

3.1.9 registrera granskningar, undantag, avvikelser, korrigerande åtgärder, revisionsiakttagelser och förbättringar i REG12.

4. Policyuttalanden

4.1 Inventering, ändamål och godkännande av övervakning

4.1.1 [Controller] Process Owner / Business Owner MUST registrera varje CCTV-aktivitet, besöksövervakning, logg över fysisk tillträdeskontroll eller fysisk övervakningsaktivitet i REG02 innan aktiviteten inleds.

4.1.2 [Controller] Privacy Lead / PIMS Manager MUST validera REG02-posten avseende ändamål, rättslig grund, övervakad plats, PII-kategorier, kategorier av registrerade, bevarande, information, åtkomst och fält för utlämnande innan en ny eller väsentligt ändrad övervakningsaktivitet aktiveras.

4.1.3 [Controller] Process Owner / Business Owner MUST registrera godkända övervakade zoner, undantagna zoner och insamlingsgränser i REG02 innan kameror, sensorer, besöksloggar eller loggning av åtkomstkontroll aktiveras.

4.1.4 [Conditional] Process Owner / Business Owner MUST inhämta ett beslut om integritetsrisk i REG04 innan övervakning aktiveras som omfattar systematisk övervakning, ljudinspelning, biometrisk identifiering, analysbaserad detektering, känsliga platser, sårbara personer eller övervakning som inte är uppenbar.

4.1.5 [Joint Controller] Privacy Lead / PIMS Manager MUST registrera ansvarsfördelning för gemensam övervakning i REG08 innan delad övervakning med hyresvärd, fastighetspartner, kund eller annan gemensamt personuppgiftsansvarig inleds.

4.1.6 [Processor] Privacy Lead / PIMS Manager MUST registrera kundinstruktioner för övervakning och tillåtna behandlingsgränser i REG08 innan övervakningsmaterial, besöksregister eller loggar över fysiskt tillträde behandlas på uppdrag av en kund.

4.2 Information och transparens

4.2.1 [Controller] Process Owner / Business Owner MUST säkerställa att underlag för övervakningsskyltning eller motsvarande just-in-time-information registreras i REG07 innan övervakade områden öppnas för registrerade.

4.2.2 [Controller] Privacy Lead / PIMS Manager MUST koppla varje integritetsmeddelande om övervakning i REG07 till motsvarande behandlingsändamål i REG02 innan publicering eller väsentlig ändring.

4.2.3 [Processor] Privacy Lead / PIMS Manager MUST tillhandahålla stödjande information för övervakningsmeddelanden i REG08 när organisationen driver övervakningstjänster enligt kundinstruktioner.

4.2.4 [Conditional] Process Owner / Business Owner MUST registrera alternativa transparensåtgärder i REG07 och REG04 innan övervakning som inte är uppenbar eller övervakning i nödsituation aktiveras.

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Undantag

9.1 [All] Privacy Lead / PIMS Manager MUST registrera varje undantag från denna policy i REG12 innan undantaget används.

9.2 [Conditional] Data Protection Officer / Privacy Advisor MUST dokumentera integritetsrådgivning i REG04 eller REG12 före godkännande av undantag som avser övervakning som inte är uppenbar, ljudinspelning, biometrisk identifiering, analysaktiverad övervakning eller känsliga övervakningsplatser.

9.3 [All] Top Management MUST godkänna undantag som överstiger 90 dagar i REG12 innan förlängning utöver den ursprungliga undantagsperioden.

9.4 [All] Privacy Lead / PIMS Manager MUST granska öppna övervakningsundantag i REG12 minst månadsvis tills de stängs.

10. Tillämpning av policyn

10.1 [All] Privacy Lead / PIMS Manager MUST registrera brister i övervakningskontroller som avvikelser i REG12 inom fem arbetsdagar efter bekräftelse.

10.2 [Both] Information Security Lead MUST stänga av obehörig åtkomst till övervakningssystem inom en arbetsdag efter bekräftelse och registrera åtgärden i REG10 eller REG12.

10.3 [All] Top Management MUST tilldela ägarskap för korrigerande åtgärder i REG12 inom 10 arbetsdagar vid upprepade eller väsentliga policyöverträdelser.

10.4 [Conditional] Incident Response Coordinator MUST initiera arbetsflödet för PII-incidenter i REG10 vid misstänkt obehörigt utlämnande, förlust eller kompromettering av övervaknings-PII.

11. Granskning och underhåll

11.1 [All] Privacy Lead / PIMS Manager MUST granska denna policy och relaterat övervakningsunderlag i REG12 minst årligen.

11.2 [Controller] Process Owner / Business Owner MUST revalidera varje aktivt övervakningsändamål, information, platsomfattning och bevarandepost i REG02 och REG07 minst årligen.

11.3 [Both] System Owner / Application Owner MUST revalidera åtkomst, loggning, radering och exportkontroller för övervakningssystem i REG12 minst årligen och efter väsentlig systemändring.

11.4 [Conditional] Vendor / Procurement Owner MUST revalidera underlag för outsourcade övervakningsleverantörer i REG08 minst årligen och före avtalsförnyelse.

11.5 [All] Privacy Lead / PIMS Manager MUST uppdatera relaterat underlag i REG02, REG04, REG07, REG08, REG10 eller REG12 inom 30 kalenderdagar efter godkända policyändringar.

12. Relaterade policyer

12.1 PII02 - Policy för integritetsroller, ansvar och ansvarsskyldighet

12.2 PII03 - Policy för inventering av PII-behandling och rättslig grund

12.3 PII04 - Policy för integritetsmeddelanden och transparens

12.4 PII06 - Policy för hantering av registrerades rättigheter

12.5 PII07 - Policy för bedömning av integritetsrisker och DPIA

12.6 PII08 - Policy för inbyggt dataskydd och dataskydd 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 hantering av personuppgiftsbiträden, underbiträden och tredjepartsintegritet

12.10 PII13 - Policy för internationell överföring av PII

12.11 PII14 - Policy för PII-säkerhet och åtkomstkontroll

12.12 PII15 - Policy för hantering av PII-incidenter och personuppgiftsincidenter

12.13 PII17 - Policy för dokumenterad information och underlagshantering i PIMS

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

12.15 PII19 - Integritetspolicy för anställda

12.16 PII21 - Integritetspolicy för AI och automatiserat beslutsfattande

12.17 PII23 - Policy för PII-personuppgiftsbiträden i molntjänster

13. Referensstandarder och ramverk

13.1 Denna policy är mappad mot följande standarder och regelverk. Mappningen förklarar hur policyn stödjer de angivna kraven och identifierar de interna klausuler som implementerar eller stödjer dem.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Mappas till dokumenterat övervakningsunderlag, operativ planering, aktiveringskontroller, ändamålsregister, informationskoppling, åtkomstkonfiguration, bevarandekonfiguration och ändringsstyrning för CCTV och fysiska övervakningsaktiviteter. 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** - Mappas till mätning av övervakningskontroller, leverantörsgranskning, åtkomstgranskning, revisionsiakttagelser, avvikelser, korrigerande åtgärder, eskalering av försenade åtgärder och förbättringsunderlag. 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** - Mappas till den personuppgiftsansvariges definition av övervakningsändamål, dokumentation av rättslig grund, beslut om utlösare för integritetsrisker och register över behandlingsaktiviteter för övervakning i REG02 och 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** - Mappas till fördelning av outsourcade övervakningsleverantörer, ansvarsfördelning vid gemensam övervakning och underlag i REG08 för personuppgiftsbiträde eller gemensamt personuppgiftsansvariga. 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** - Mappas till övervakningsrelaterade skyldigheter gentemot registrerade, dirigering av begäranden, bevarande som behövs för att bedöma begäranden och styrningsunderlag för stöd till rättigheter. 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** - Mappas till begränsning av övervakningsinsamling, behandlingsgränser, minimering, bevarandeperioder, radering, överskrivning, bevarandespärrar och kontroll av extraherade kopior. 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** - Mappas till register över externt utlämnande, hantering av begäranden om utlämnande, minimering före utlämnande och incidentkopplade utlämnanden som omfattar övervaknings-PII. 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** - Mappas till personuppgiftsbiträdets kundinstruktioner, tillåtna behandlingsgränser, informationsstöd, instruktioner om bevarande och radering, stöd vid rättigheter och register för outsourcade övervakningstjänster. 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** - Mappas till personuppgiftsbiträdets stöd för kundens skyldigheter, godkännande av utlämnande, register över utlämnanden, underrättelse om begäranden om utlämnande och hantering av rättsligt bindande utlämnanden av övervaknings-PII. 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** - Mappas till skydd av övervakningsregister, begränsad åtkomst, granskning av privilegierad åtkomst, åtkomstloggning, begränsning av obehörig åtkomst och loggningsunderlag för övervakningssystem. 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)** - Mappas till laglighet, korrekthet, transparens, ändamålsbegränsning, uppgiftsminimering,

lagringsminimering och ansvarsskyldighetsunderlag för övervakningsaktiviteter. 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 - Mappas till dokumentation av rättslig grund för CCTV, besöksövervakning, loggar över fysiskt tillträde och andra fysiska övervakningsaktiviteter. Addressed by clauses [4.1.2; 4.1.4; 7.1].

13.3.3 **Article 12; Article 13; Article 14** - Mappas till transparenta övervakningsmeddelanden, skyltunderlag, koppling av information till behandlingsändamål, personuppgiftsbiträdets stödjande information för meddelanden och alternativa transparensåtgärder. 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** - Mappas till tillgång, rättelse, radering, begränsning, invändning, dirigering av begäranden, bevarande som behövs för att bedöma begäranden och övervakningsrelaterat kundstöd. 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** - Mappas till den personuppgiftsansvariges styrning, fördelning mellan gemensamt personuppgiftsansvariga, styrning av personuppgiftsbiträden, register över behandling, säkerhet i övervakningssystem, granskning av integritetsrisker, DPIA-utlösare och integritetsrådgivning. 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** - Mappas till ändamålsspecificering, insamlingsbegränsning, uppgiftsminimering, användningsbegränsning, bevarandebegränsning och begränsning av utlämnande för övervaknings-PII. 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** - Mappas till transparens, individens deltagande, ansvarsskyldighet, informationssäkerhet, efterlevnadsgranskning, åtkomstgranskning, dirigering av rättigheter, incidenteskalering och underlag för korrigerande åtgärder. 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** - Mappas till screening av integritetsrisker och DPIA-utlösare för systematisk, icke-uppenbar, ljudbaserad, biometrisk, analysaktiverad, platskänslig, sårbarhetsrelaterad eller annan fysisk övervakning med högre risk. 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** - Mappas till dataskyddskontroller för PII avseende ändamål, insamling, minimering, bevarande, utlämnande och registrerades deltagande i övervakningssammanhang. 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** - Mappas till åtkomsttilldelning, begränsning av informationsåtkomst och kontroller för fysiskt tillträde som är relevanta för åtkomst till övervakningssystem och register från fysisk tillträdeskontroll. 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 - Mappas till integritet och skydd av PII, fysiskt tillträde, fysisk säkerhetsövervakning, privilegierad åtkomst, begränsning av informationsåtkomst och loggningskontroller för CCTV och fysiska övervakningssystem. 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].