					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: PII24					Titlul documentului: **Politica de confidențialitate privind CCTV și monitorizarea fizică**							
Versiunea: 1.0		Data intrării în vigoare: 01.01.2025			Proprietarul documentului:							
X	Politică		Standard		Procedură		Formular		Registru		Altul	

Istoricul reviziilor				
Numărul reviziei	**Data reviziei**	**Modificări**	**Revizuit de**	**Proprietarul procesului**

Aprobări			
Nume	**Funcție**	**Data**	**Semnătură**

Aliniată la standardele și reglementările aplicabile

Standard/reglementare	Clauză/control/articol	Aplicabilitate	Tip de acoperire	Comentariu
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Controale documentate și operaționale
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorizare și acțiune corectivă
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	Scop, temei juridic, declanșator de risc și înregistrări
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Alocarea către persoana împuternicită și operatorul asociat
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	Obligații și cereri ale persoanei vizate
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	Colectare, prelucrare, minimizare, retenție și eliminare
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Înregistrări și cereri privind divulgarea
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	Acorduri, instrucțiuni, suport și înregistrări ale persoanei împuternicite
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	Drepturi și suport pentru divulgare acordate de persoana împuternicită
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Protecția înregistrărilor și jurnalizare
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Principii și responsabilitate
GDPR	Article 6	Controller	Primary	Temei juridic

GDPR	Article 12; Article 13; Article 14	Controller	Primary	Transparență și note de informare
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21	Controller	Supporting	Cereri de exercitare a drepturilor
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Guvernanță, persoane împuternicite, înregistrări, securitate, DPIA și consiliere
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Scop, colectare, minimizare, retenție și divulgare
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Transparență, participare, responsabilitate, securitate și conformitate
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Risc privind confidențialitatea și declanșatoare DPIA
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Controale de confidențialitate pentru protecția PII
ISO/IEC 29151:2022	Clause 9.2.3; Clause 9.4.2; Clause 11.1.3	Both	Supporting	Controale privind accesul și intrarea fizică
ISO/IEC 27002:2022	Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15	Both	Supporting	PII, monitorizare fizică, restricționarea accesului și jurnalizare

1. Domeniu de aplicare

1.1 Această politică se aplică CCTV, monitorizării video, monitorizării vizitatorilor, jurnalelor de control al accesului fizic, înregistrărilor de monitorizare operate de personalul de pază, sistemelor de monitorizare a spațiilor și activităților conexe de monitorizare fizică prin care se colectează sau se prelucrează în alt mod PII.

1.2 Această politică se aplică organizațiilor care acționează ca operatori PII pentru propriile spații și activități de monitorizare fizică. Se aplică, de asemenea, activităților de suport desfășurate ca persoană împuternicită sau persoană subîmputernicită atunci când organizația operează, găzduiește, revizuiește, stochează, divulgă, șterge sau prelucrează în alt mod înregistrări video de monitorizare, date ale vizitatorilor sau jurnale de acces fizic în numele unui client.

1.3 Această politică acoperă definirea scopului monitorizării, aprobarea, notele de informare și semnalizarea, restricțiile de acces, divulgarea, retenția, ștergerea, externalizarea, escaladarea incidentelor, direcționarea cererilor de exercitare a drepturilor, revizuirea și gestionarea dovezilor.

1.4 Această politică nu oferă consultanță privind dreptul muncii, comentarii juridice privind consiliile angajaților, proceduri pentru organele de aplicare a legii sau un registru CCTV dedicat. Dovezile specifice monitorizării sunt menținute în obiectele canonice de dovezi PIMS identificate în această politică.

2. Scop

2.1 Scopul acestei politici este de a stabili controale de confidențialitate pentru CCTV și monitorizarea fizică, astfel încât activitățile de monitorizare să aibă un scop definit, să fie transparente, proporționale, controlate din perspectiva accesului, păstrate pe perioade definite, divulgate numai prin canale aprobate și susținute de dovezi PIMS care pot fi auditate.

2.2 Această politică sprijină gestionarea consecventă a înregistrărilor video de monitorizare, a înregistrărilor privind vizitatorii, a jurnalelor de acces fizic și a PII conexe monitorizării, fără a crea registre, comitete, tablouri de bord sau roluri necanonice suplimentare.

3. Obiective

3.1 Obiectivele acestei politici sunt:

3.1.1 să definească scopurile monitorizării și domeniul prelucrării înainte de începerea monitorizării;

3.1.2 să documenteze în REG02 activitățile CCTV, de acces fizic, de monitorizare a vizitatorilor și de monitorizare fizică;

3.1.3 să identifice în REG04 activitățile de monitorizare care necesită revizuirea riscurilor privind confidențialitatea sau evaluare preliminară DPIA;

3.1.4 să mențină în REG07 dovezi transparente privind notele de informare și semnalizarea;

3.1.5 să restricționeze accesul, vizualizarea, exportul, divulgarea și retenția PII de monitorizare;

3.1.6 să direcționeze cererile persoanelor vizate prin REG06;

3.1.7 să gestioneze furnizorii de monitorizare externalizați și dovezile privind partajarea datelor prin REG08;

3.1.8 să escaladeze prin REG10 incidentele PII suspectate, legate de monitorizare;

3.1.9 să înregistreze în REG12 revizuirile, excepțiile, neconformitățile, acțiunile corective, constatările de audit și îmbunătățirile.

4. Declarații de politică

4.1 Inventarul, scopul și aprobarea monitorizării

4.1.1 [Controller] Process Owner / Business Owner MUST înregistra fiecare activitate CCTV, de monitorizare a vizitatorilor, fiecare jurnal de control al accesului fizic sau fiecare activitate de monitorizare fizică în REG02 înainte de începerea activității.

4.1.2 [Controller] Privacy Lead / PIMS Manager MUST valida înregistrarea din REG02 privind scopul, temeiul juridic, locația monitorizată, categoriile de PII, categoriile de persoane vizate, retenția, nota de informare, accesul și câmpurile privind divulgarea înainte de activarea unei activități de monitorizare noi sau modificate semnificativ.

4.1.3 [Controller] Process Owner / Business Owner MUST înregistra în REG02 zonele monitorizate aprobate, zonele excluse și limitele colectării înainte de activarea camerelor, senzorilor, jurnalelor de vizitatori sau jurnalizării controlului accesului.

4.1.4 [Conditional] Process Owner / Business Owner MUST obține o decizie privind riscul de confidențialitate în REG04 înainte de activarea monitorizării care implică monitorizare sistematică, înregistrare audio, identificare biometrică, detecție bazată pe analiză, locații sensibile, persoane vulnerabile sau monitorizare care nu este evidentă.

4.1.5 [Joint Controller] Privacy Lead / PIMS Manager MUST înregistra în REG08 alocarea responsabilităților pentru monitorizarea comună înainte de începerea monitorizării partajate cu un proprietar al clădirii, partener de facilități, client sau alt operator asociat.

4.1.6 [Processor] Privacy Lead / PIMS Manager MUST înregistra în REG08 instrucțiunile clientului privind monitorizarea și limitele permise ale prelucrării înainte de prelucrarea în numele unui client a înregistrărilor video de monitorizare, a înregistrărilor privind vizitatorii sau a jurnalelor de acces fizic.

4.2 Note de informare și transparență

4.2.1 [Controller] Process Owner / Business Owner MUST se asigure că dovezile privind semnalizarea de monitorizare sau notele de informare echivalente la momentul colectării sunt înregistrate în REG07 înainte ca zonele monitorizate să fie deschise persoanelor vizate.

4.2.2 [Controller] Privacy Lead / PIMS Manager MUST corela fiecare notă de informare privind monitorizarea din REG07 cu scopul de prelucrare corespunzător din REG02 înainte de publicare sau de o modificare semnificativă.

4.2.3 [Processor] Privacy Lead / PIMS Manager MUST furniza în REG08 informații-suport pentru notele de informare privind monitorizarea atunci când organizația operează servicii de monitorizare conform instrucțiunilor clientului.

4.2.4 [Conditional] Process Owner / Business Owner MUST înregistra măsuri alternative de transparență în REG07 și REG04 înainte de activarea monitorizării care nu este evidentă sau a monitorizării de urgență.

[... Secțiunile 4.3–8 nu sunt incluse în această previzualizare. Achiziționați documentul complet pentru a accesa conținutul integral. ...]

9. Excepții

9.1 [All] Privacy Lead / PIMS Manager MUST înregistra fiecare excepție de la această politică în REG12 înainte ca excepția să fie utilizată.

9.2 [Conditional] Data Protection Officer / Privacy Advisor MUST documenta consilierea privind confidențialitatea în REG04 sau REG12 înainte de aprobarea excepțiilor care implică monitorizare care nu este evidentă, înregistrare audio, identificare biometrică, monitorizare bazată pe analiză sau locații sensibile de monitorizare.

9.3 [All] Top Management MUST aproba în REG12 excepțiile care depășesc 90 de zile înainte de prelungirea peste perioada inițială a excepției.

9.4 [All] Privacy Lead / PIMS Manager MUST revizui în REG12 excepțiile deschise privind monitorizarea cel puțin lunar până la închidere.

10. Aplicare

10.1 [All] Privacy Lead / PIMS Manager MUST înregistra deficiențele controalelor de monitorizare ca neconformități în REG12 în termen de cinci zile lucrătoare de la confirmare.

10.2 [Both] Information Security Lead MUST suspenda accesul neautorizat la sistemul de monitorizare în termen de o zi lucrătoare de la confirmare și trebuie să înregistreze acțiunea în REG10 sau REG12.

10.3 [All] Top Management MUST atribui în REG12 responsabilitatea pentru acțiunea corectivă în termen de 10 zile lucrătoare pentru încălcări repetate sau semnificative ale politicii.

10.4 [Conditional] Incident Response Coordinator MUST iniția fluxul de lucru pentru incidente PII în REG10 la suspiciunea unei divulgări neautorizate, pierderi sau compromiteri a PII de monitorizare.

11. Revizuire și întreținere

11.1 [All] Privacy Lead / PIMS Manager MUST revizui această politică și dovezile aferente monitorizării în REG12 cel puțin anual.

11.2 [Controller] Process Owner / Business Owner MUST revalida fiecare scop activ al monitorizării, fiecare notă de informare, domeniul locației și înregistrarea de retenție în REG02 și REG07 cel puțin anual.

11.3 [Both] System Owner / Application Owner MUST revalida în REG12 controalele privind accesul la sistemul de monitorizare, jurnalizarea, ștergerea și exportul cel puțin anual și după o modificare semnificativă a sistemului.

11.4 [Conditional] Vendor / Procurement Owner MUST revalida dovezile privind furnizorii de monitorizare externalizați în REG08 cel puțin anual și înainte de reînnoirea contractului.

11.5 [All] Privacy Lead / PIMS Manager MUST actualiza dovezile conexe din REG02, REG04, REG07, REG08, REG10 sau REG12 în termen de 30 de zile calendaristice de la modificările aprobate ale politicii.

12. Politici conexe

12.1 PII02 - Politica privind rolurile, responsabilitățile și responsabilitatea pentru confidențialitate

12.2 PII03 - Politica privind inventarul prelucrării PII și temeiul juridic

12.3 PII04 - Politica privind notele de informare și transparența în materie de confidențialitate

12.4 PII06 - Politica de gestionare a drepturilor persoanelor vizate

12.5 PII07 - Politica de evaluare a riscurilor privind confidențialitatea și DPIA

12.6 PII08 - Politica privind protecția datelor încă din faza de proiectare și în mod implicit

12.7 PII09 - Politica privind colectarea, utilizarea, divulgarea și partajarea PII

12.8 PII10 - Politica privind retenția, ștergerea și eliminarea PII

12.9 PII12 - Politica privind managementul confidențialității pentru persoanele împuternicite, persoanele subîmputernicite și terți

12.10 PII13 - Politica privind transferul internațional de PII

12.11 PII14 - Politica privind securitatea PII și controlul accesului

12.12 PII15 - Politica de gestionare a incidentelor și încălcărilor privind PII

12.13 PII17 - Politica privind informațiile documentate și gestionarea dovezilor PIMS

12.14 PII18 - Politica privind monitorizarea, auditul și îmbunătățirea PIMS

12.15 PII19 - Politica privind confidențialitatea angajaților

12.16 PII21 - Politica de confidențialitate privind AI și proces decizional automatizat

12.17 PII23 - Politica privind persoana împuternicită pentru PII în cloud

13. Standarde și cadre de referință

13.1 Această politică este mapată la următoarele standarde și reglementări. Maparea explică modul în care politica susține cerințele citate și identifică clauzele interne care le implementează sau le sprijină.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Mapate la dovezile documentate privind monitorizarea, planificarea operațională, controalele de activare, înregistrările privind scopul, corelarea cu notele de informare, configurarea accesului, configurarea retenției și controlul modificărilor pentru activitățile CCTV și de monitorizare fizică. 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** - Mapate la măsurarea controalelor de monitorizare, revizuirea furnizorilor, revizuirea accesului, constatările de audit, neconformitățile, acțiunile corective, escaladarea acțiunilor restante și dovezile de îmbunătățire. 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** - Mapate la definirea de către operator a scopului monitorizării, documentarea temeiului juridic, deciziile privind declanșatoarele riscului de confidențialitate și evidențele activităților de prelucrare aferente monitorizării în REG02 și 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** - Mapate la alocarea furnizorilor de monitorizare externalizată, alocarea responsabilităților pentru monitorizarea comună și dovezile privind persoana împuternicită sau operatorul asociat în 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** - Mapate la obligațiile față de persoana vizată legate de monitorizare, direcționarea cererilor, păstrarea necesară pentru evaluarea cererilor și dovezile de guvernanță pentru suportul privind drepturile. 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** - Mapate la limitarea colectării prin monitorizare, limitele prelucrării, minimizare, perioade de retenție, ștergere, suprascriere, blocări pentru păstrare și controlul copiilor extrase. 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** - Mapate la evidențele divulgării externe, gestionarea cererilor de divulgare, minimizarea înainte de divulgare și divulgările legate de incidente care implică PII de monitorizare. 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** - Mapate la instrucțiunile clientului pentru persoana împuternicită, limitele permise ale prelucrării, suportul pentru notele de informare, instrucțiunile privind retenția și ștergerea, asistența privind drepturile și înregistrările persoanei împuternicite pentru serviciile de monitorizare externalizate. 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** - Mapate la suportul persoanei împuternicite pentru obligațiile clientului, autorizarea divulgării, evidențele divulgării, notificarea cererilor de divulgare și gestionarea divulgărilor cu caracter obligatoriu din punct de vedere juridic pentru PII de monitorizare. 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** - Mapate la protecția înregistrărilor de monitorizare, accesul restricționat, revizuirea accesului privilegiat, jurnalizarea accesului, conținerea accesului

neautorizat și dovezile de jurnalizare pentru sistemele de monitorizare. 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)** - Mapate la legalitate, echitate, transparență, limitarea scopului, minimizarea datelor, limitarea stocării și dovezile de responsabilitate pentru activitățile de monitorizare. 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 - Mapat la documentarea temeiului juridic pentru CCTV, monitorizarea vizitatorilor, jurnalele de acces fizic și alte activități de monitorizare fizică. Addressed by clauses [4.1.2; 4.1.4; 7.1].

13.3.3 **Article 12; Article 13; Article 14** - Mapate la note de informare transparente privind monitorizarea, dovezi privind semnalizarea, corelarea notelor de informare cu scopurile prelucrării, informații-suport pentru notele de informare furnizate de persoana împuternicită și măsuri alternative de transparență. 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** - Mapate la acces, rectificare, ștergere, restricționare, opoziție, direcționarea cererilor, păstrarea necesară pentru evaluarea cererilor și asistența acordată clientului în legătură cu monitorizarea. 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** - Mapate la guvernanța operatorului, alocarea către operatorul asociat, guvernanța persoanei împuternicite, evidențele activităților de prelucrare, securitatea sistemelor de monitorizare, revizuirea riscurilor privind confidențialitatea, declanșatoarele DPIA și consilierea privind confidențialitatea. 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** - Mapate la specificarea scopului, limitarea colectării, minimizarea datelor, limitarea utilizării, limitarea retenției și limitarea divulgării pentru PII de monitorizare. 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** - Mapate la transparență, participare individuală, responsabilitate, securitatea informațiilor, revizuirea conformității, revizuirea accesului, direcționarea cererilor de exercitare a drepturilor, escaladarea incidentelor și dovezile privind acțiunile corective. 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** - Mapate la evaluarea riscului privind confidențialitatea și evaluarea preliminară a declanșatoarelor DPIA pentru monitorizare fizică sistematică, care nu este evidentă, audio, biometrică, bazată pe analiză, în locații sensibile, care implică persoane vulnerabile sau altă monitorizare fizică cu risc mai ridicat. 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** - Mapate la controale de protecție a PII pentru scop, colectare, minimizare, retenție, divulgare și participarea persoanei vizate în contexte de monitorizare. 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** - Mapate la acordarea accesului, restricționarea accesului la informații și controalele de intrare fizică relevante pentru accesul la sistemele de monitorizare și înregistrările de control al accesului fizic. 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 - Mapate la confidențialitatea și protecția PII, intrarea fizică, monitorizarea securității fizice, accesul privilegiat, restricționarea accesului la informații și controalele de jurnalizare pentru sistemele CCTV și de monitorizare fizică. 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].