					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: PII16					Titlul documentului: **Politica privind instruirea, conștientizarea și competența în domeniul confidențialității**							
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 acoperire	Comentariu
ISO/IEC 27701:2025	Clause 7.2; Clause 7.3	Both	Primary	Competență și conștientizare
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Comunicare și dovezi documentate
ISO/IEC 27701:2025	Clause 8.1; Clause 9.1; Clause 10.2	Both	Supporting	Control operațional, măsurare și îmbunătățire
ISO/IEC 27701:2025	Annex A.3.17	Both	Primary	Conștientizare, educare și instruire privind prelucrarea PII
GDPR	Article 5(2); Article 24; Article 28; Article 32; Article 39	Both	Supporting	Responsabilitate, guvernanța persoanelor împuternicite, securitate și atribuțiile DPO
ISO/IEC 27001:2022	Clause 7.2; Clause 7.3; Annex A control 6.3	Both	Supporting	Competență, conștientizare și instruire
ISO/IEC 27002:2022	Control 6.3	Both	Supporting	Îndrumări privind conștientizarea, educarea și instruirea
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Securitatea informațiilor și conformitatea privind confidențialitatea

1. Domeniu de aplicare

1.1 Această politică definește cerințele organizației privind instruirea, conștientizarea și competența în domeniul confidențialității în cadrul Sistemului de management al informațiilor privind confidențialitatea.

1.2 Această politică se aplică personalului, contractorilor, personalului temporar, părților terțe relevante, persoanelor împuternicite, persoanelor subîmputernicite și altor părți interesate a căror activitate poate afecta prelucrarea PII, performanța PIMS, drepturile persoanelor vizate, riscul privind confidențialitatea, securitatea informațiilor aferentă PII, instrucțiunile persoanelor împuternicite, incidentele privind confidențialitatea, informațiile documentate sau dovezile de conformitate.

1.3 Această politică se aplică în contexte de operator, operator asociat, persoană împuternicită și persoană subîmputernicită.

1.4 Această politică acoperă următoarele:

1.4.1 identificarea publicului-țintă al instruirii privind confidențialitatea;

1.4.2 instruirea la integrare;

1.4.3 instruirea anuală de reîmprospătare;

1.4.4 instruirea bazată pe roluri și instruirea declanșată de evenimente;

1.4.5 dovezile privind finalizarea instruirii;

1.4.6 escaladarea nefinalizării;

1.4.7 revizuirea eficacității instruirii;

1.4.8 dovezile privind asigurarea instruirii persoanelor împuternicite, a persoanelor subîmputernicite și a terților.

1.5 Această politică nu creează o matrice separată de instruire, un tablou de bord al instruirii, un registru de resurse umane, un registru de competențe, un registru disciplinar sau un registru de instruire a clienților. Atribuirile de instruire, finalizările, reamintirile, dovezile de competență și dovezile de conștientizare sunt înregistrate în REG11, iar excepțiile, escaladările, neconformitățile, acțiunile corective și dovezile de revizuire sunt înregistrate în REG12. Dovezile privind asigurarea instruirii persoanelor împuternicite, a persoanelor subîmputernicite și a terților sunt înregistrate în REG08, după caz.

1.6 Această politică nu dublează următoarele:

1.6.1 atribuirea responsabilităților aferente rolurilor din PII02;

1.6.2 cerințele privind inventarul prelucrărilor și temeiul juridic din PII03;

1.6.3 metodologia privind riscurile de confidențialitate și DPIA din PII07;

1.6.4 punctele de control pentru protecția datelor încă din faza de proiectare din PII08;

1.6.5 guvernanța ciclului de viață al persoanelor împuternicite din PII12;

1.6.6 operarea securității PII și a controlului accesului din PII14;

1.6.7 fluxul de lucru pentru incidente și încălcări privind PII din PII15;

1.6.8 guvernanța informațiilor documentate din PII17;

1.6.9 guvernanța monitorizării, auditului intern și îmbunătățirii din PII18.

2. Scop

2.1 Scopul acestei politici este să asigure că persoanele a căror activitate afectează prelucrarea PII își înțeleg responsabilitățile privind confidențialitatea, finalizează instruirea adecvată la o cadență definită, mențin competența relevantă pentru rol și generează dovezi auditabile privind instruirea, conștientizarea și escaladarea.

2.2 Această politică susține implementarea consecventă a PIMS prin utilizarea REG11 ca obiect principal de dovezi pentru instruire și conștientizare și a REG08, REG10 și REG12 ca obiecte de dovezi suport.

3. Obiective

3.1 Obiectivele acestei politici sunt:

3.1.1 să definească publicurile-țintă ale instruirii privind confidențialitatea;

3.1.2 să definească cerințele privind instruirea la integrare;

3.1.3 să definească cerințele privind instruirea anuală de reîmprospătare;

3.1.4 să definească cerințele privind instruirea în domeniul confidențialității bazată pe roluri;

3.1.5 să înregistreze dovezile de finalizare în REG11;

3.1.6 să escaladeze nefinalizarea prin REG12;

3.1.7 să mențină în REG08 dovezile privind asigurarea instruirii persoanelor împuternicite, a persoanelor subîmputernicite și a terților, după caz;

3.1.8 să revizuiască eficacitatea instruirii fără a crea metrici excesive sau registre duplicate;

3.1.9 să asigure că materialele de instruire rămân aliniate la politicile PIMS curente și la obligațiile semnificative privind confidențialitatea.

4. Declarații de politică

4.1 Publicul-țintă și atribuirea instruirii

4.1.1 [All] Privacy Lead / PIMS Manager TREBUIE SĂ definească în REG11 categoriile de public-țintă al instruirii PIMS înainte de începerea fiecărui ciclu anual de instruire.

4.1.2 [All] Process Owner / Business Owner TREBUIE SĂ identifice în REG11 personalul ale cărui atribuții implică prelucrarea PII înainte de integrare, atribuirea rolului sau modificarea semnificativă a atribuțiilor.

4.1.3 [Conditional] System Owner / Application Owner TREBUIE SĂ identifice în REG11 utilizatorii care necesită instruire privind confidențialitatea pentru sisteme PII, acces privilegiat sau administrare înainte ca accesul să fie activat sau modificat semnificativ.

4.1.4 [Joint Controller] Privacy Lead / PIMS Manager TREBUIE SĂ înregistreze alocarea responsabilităților de instruire ale operatorilor asociați în REG11 sau REG08 înainte ca activitatea de prelucrare comună să înceapă sau să se modifice semnificativ.

4.1.5 [Conditional] Data Protection Officer / Privacy Advisor TREBUIE SĂ identifice în REG11 nevoile de instruire aprofundată privind confidențialitatea înainte ca instruirea să fie atribuită rolurilor care gestionează prelucrări cu risc ridicat, PII din categorii speciale, drepturile persoanelor vizate, DPIA, transferuri internaționale sau evaluarea încălcării securității datelor.

4.1.6 [All] Privacy Lead / PIMS Manager TREBUIE SĂ înregistreze în REG11 publicul-țintă al instruirii atribuit, tipul de instruire, data obligatorie de finalizare și proprietarul dovezilor înainte de începerea fiecărui ciclu anual de instruire.

4.2 Cadența instruirii la integrare și a instruirii anuale

4.2.1 [All] Privacy Lead / PIMS Manager TREBUIE SĂ atribuie în REG11 instruirea de bază privind conștientizarea confidențialității în termen de 10 zile lucrătoare de la integrare pentru personalul cu acces la PII sau cu responsabilități PIMS.

4.2.2 [All] Process Owner / Business Owner TREBUIE SĂ asigure că personalul desemnat finalizează instruirea privind confidențialitatea la integrare în REG11 înainte ca accesul nesupravegheat la PII să fie aprobat sau în termen de 30 de zile de la integrare, oricare dintre acestea survine mai întâi.

4.2.3 [All] Privacy Lead / PIMS Manager TREBUIE SĂ atribuie în REG11 instruirea anuală de reîmprospătare privind confidențialitatea cel puțin o dată la fiecare 12 luni.

4.2.4 [All] Process Owner / Business Owner TREBUIE SĂ confirme în REG11 stadiul finalizării instruirii anuale de reîmprospătare pentru personalul atribuit până la termenul anual publicat.

4.2.5 [Conditional] Privacy Lead / PIMS Manager TREBUIE SĂ atribuie în REG11 instruire specifică de reîmprospătare în termen de 30 de zile după o modificare semnificativă a politicii privind confidențialitatea, o modificare semnificativă a procesului PIMS, o constatare de audit, un eșec recurent al instruirii sau o lecție relevantă rezultată dintr-un incident PII.

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

9. Excepții

9.1.1 [All] Process Owner / Business Owner TREBUIE SĂ înregistreze în REG12 o solicitare de excepție privind instruirea în domeniul confidențialității înainte ca un termen obligatoriu de finalizare să fie prelungit.

9.1.2 [All] Privacy Lead / PIMS Manager TREBUIE SĂ aprobe sau să respingă în REG12 solicitările de excepție privind instruirea în domeniul confidențialității înainte ca excepția să devină activă.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor TREBUIE SĂ ofere consiliere privind excepțiile de instruire în REG12 înainte de aprobare atunci când excepția afectează prelucrări cu risc ridicat, PII din categorii speciale, gestionarea drepturilor, gestionarea incidentelor, transferurile internaționale sau dovezile de certificare.

9.1.4 [Conditional] Top Management TREBUIE SĂ aprobe în REG12 excepțiile privind instruirea în domeniul confidențialității înainte de activare atunci când excepția afectează nefinalizarea repetată, accesul privilegiat la PII, prelucrarea PII cu impact ridicat sau dovezile destinate autorităților de reglementare.

9.1.5 [All] Privacy Lead / PIMS Manager TREBUIE SĂ definească în REG12 proprietarul excepției, data expirării, acțiunea compensatorie și data revizuirii înainte de aprobarea oricărei excepții privind instruirea în domeniul confidențialității.

9.1.6 [All] Process Owner / Business Owner TREBUIE SĂ închidă sau să reînnoiască în REG12 excepțiile aprobate privind instruirea în domeniul confidențialității înainte de data expirării excepției.

10. Aplicare

10.1.1 [All] Privacy Lead / PIMS Manager TREBUIE SĂ înregistreze în REG12 o neconformitate de instruire în termen de cinci zile lucrătoare atunci când dovezile instruirii obligatorii privind confidențialitatea lipsesc, sunt incomplete, sunt restante sau nu sunt trasabile la REG11.

10.1.2 [All] Process Owner / Business Owner TREBUIE SĂ asigure că instruirea obligatorie privind confidențialitatea restantă este finalizată sau escaladată în REG11 sau REG12 în termen de 10 zile lucrătoare după înregistrarea stadiului de întârziere.

10.1.3 [Conditional] System Owner / Application Owner TREBUIE SĂ restricționeze în REG12 accesul nou la PII cu impact ridicat atunci când instruirea obligatorie la integrare sau instruirea privind confidențialitatea bazată pe roluri rămâne incompletă după escaladare.

10.1.4 [Processor] Vendor / Procurement Owner TREBUIE SĂ escaladeze în REG08 și REG12 lipsa dovezilor de asigurare privind instruirea persoanei împuternicite, a persoanei subîmputernicite sau a forței de muncă externe în termen de cinci zile lucrătoare după identificare.

10.1.5 [Conditional] Incident Response Coordinator TREBUIE SĂ lege acțiunile de aplicare aferente instruirii de REG10 în termen de o zi lucrătoare atunci când eșecul instruirii a contribuit la un incident PII suspectat sau confirmat.

10.1.6 [All] Internal Audit / Compliance Reviewer TREBUIE SĂ verifice dovezile de închidere pentru acțiunile corective privind instruirea în REG12 la următorul audit programat sau în termen de 60 de zile de la închidere, oricare dintre acestea survine mai întâi.

11. Revizuire și mentenanță

11.1.1 [All] Privacy Lead / PIMS Manager TREBUIE SĂ revizuiască această politică și conținutul instruirii cel puțin anual și să înregistreze rezultatul revizuirii în REG11 sau REG12.

11.1.2 [All] Privacy Lead / PIMS Manager TREBUIE SĂ revizuiască această politică în termen de 30 de zile după o modificare semnificativă a domeniului de aplicare al PIMS, a legislației privind confidențialitatea, a activităților de prelucrare, a modelului de roluri, a lecțiilor din incidente, a constatărilor de audit sau a rezultatelor privind eficacitatea instruirii.

11.1.3 [Conditional] Data Protection Officer / Privacy Advisor TREBUIE SĂ revizuiască în REG12 modificările de politică semnificative din perspectiva confidențialității înainte de aprobare.

11.1.4 [All] Top Management TREBUIE SĂ aprobe în REG12 modificările semnificative ale acestei politici înainte de publicare.

11.1.5 [All] Privacy Lead / PIMS Manager TREBUIE SĂ actualizeze în REG11 conținutul instruirii și dovezile privind atribuirile în termen de 30 de zile după aprobarea unei modificări semnificative a politicii.

12. Politici conexe

12.1 Această politică trebuie citită împreună cu următoarele politici:

12.1.1 PII01 - Politica privind Sistemul de management al informațiilor privind confidențialitatea;

12.1.2 PII02 - Politica privind rolurile, responsabilitățile și răspunderea în domeniul confidențialității;

12.1.3 PII03 - Politica privind inventarul prelucrărilor PII și temeiul juridic;

12.1.4 PII04 - Politica privind notele de informare și transparența;

12.1.5 PII05 - Politica privind gestionarea consimțământului și preferințelor;

12.1.6 PII06 - Politica privind gestionarea drepturilor persoanelor vizate;

12.1.7 PII07 - Politica privind evaluarea riscurilor privind confidențialitatea și DPIA;

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

12.1.9 PII09 - Politica privind colectarea, utilizarea, divulgarea și partajarea PII;

12.1.10 PII10 - Politica privind retenția, ștergerea și eliminarea PII;

12.1.11 PII12 - Politica de management al confidențialității pentru persoane împuternicite, persoane subîmputernicite și terți;

12.1.12 PII13 - Politica privind transferul internațional de PII;

12.1.13 PII14 - Politica privind securitatea PII și controlul accesului;

12.1.14 PII15 - Politica privind managementul incidentelor și încălcărilor aferente PII;

12.1.15 PII17 - Politica PIMS privind informațiile documentate și managementul dovezilor;

12.1.16 PII18 - Politica PIMS privind monitorizarea, auditul și îmbunătățirea.

13. Standarde și cadre de referință

13.1 ISO/IEC 27701:2025 - Clause 7.2; Clause 7.3; Clause 7.4. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 7.1.1; 7.1.2; 7.1.3; 11.1.1; 11.1.5].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.4; 4.6.5; 6.1.1; 6.1.2; 6.1.3; 6.1.5; 7.1.7; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 9.1.1; 9.1.2; 9.1.5; 10.1.1; 10.1.2; 10.1.6; 11.1.1; 11.1.2; 11.1.4].

13.3 ISO/IEC 27701:2025 - Annex A.3.17. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 11.1.5].

13.4 GDPR - Article 5(2); Article 24; Article 28; Article 32; Article 39. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.4.4; 4.5.3; 4.5.4; 4.5.5; 5.1.1; 5.1.3; 5.1.7; 6.1.2; 6.1.3; 6.1.4; 7.1.4; 7.1.5; 9.1.3; 9.1.4; 10.1.3; 10.1.4; 10.1.5; 11.1.3].

13.5 ISO/IEC 27001:2022 - Clause 7.2; Clause 7.3; Annex A control 6.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.3; 4.3.1; 4.3.5; 4.4.1; 4.4.3; 4.5.1; 4.5.2; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 6.1.1; 7.1.1; 7.1.2; 8.1.1; 8.1.2; 8.1.3; 11.1.1].

13.6 ISO/IEC 27002:2022 - Control 6.3. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 10.1.2].

13.7 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.5.5; 4.6.4; 4.6.5; 5.1.3; 6.1.2; 6.1.3; 6.1.5; 8.1.5; 9.1.3; 10.1.1; 10.1.6; 11.1.2].