					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: PII02					Titlul documentului: **Politica privind rolurile, responsabilitățile și responsabilitatea 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**

Notă juridică (drepturi de autor și restricții de utilizare)

(C) 2025 Clarysec LLC. All rights reserved.

Acest document este proprietatea intelectuală a Clarysec LLC. Nicio parte a acestui document nu poate fi copiată, reutilizată, distribuită sau modificată în scopuri comerciale sau de implementare fără autorizare prealabilă expresă, în scris.

Utilizarea neautorizată este strict interzisă și poate conduce la acțiuni legale.

Pentru licențiere, contactați: info@clarysec.com

Aliniată la standardele și reglementările aplicabile

Standard / reglementare	Clauză / control / articol	Applicability	Coverage Type	Comentariu
ISO/IEC 27701:2025	Clause 4.1	Both	Primary	Contextul rolurilor PIMS
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Leadership și responsabilitate
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Roluri, responsabilități și autorități PIMS
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Competența aferentă rolurilor
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Conștientizarea rolurilor
ISO/IEC 27701:2025	Clause 7.4	Both	Supporting	Comunicarea rolurilor
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Informații documentate privind rolurile
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Deținerea controlului operațional
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Rolul de audit independent
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Revizuirea de management a responsabilității
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Neconformități și acțiuni corective legate de roluri
ISO/IEC 27701:2025	Annex A.1.2.7	Controller	Supporting	Responsabilitatea pentru contractul cu persoana împuternicită
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Primary	Rolurile și responsabilitățile operatorilor asociați
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Înregistrări privind responsabilitatea
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Primary	Acordurile și instrucțiunile clienților pentru persoana împuternicită

ISO/IEC 27701:2025	Annex A.2.2.3	Processor	Supporting	Alinierea scopurilor persoanei împuternicite
GDPR	Article 5(2)	Controller	Supporting	Dovezi privind responsabilitatea
GDPR	Article 24	Controller	Supporting	Responsabilitatea operatorului și măsuri
GDPR	Article 26	Joint Controller	Supporting	Aranjamente între operatori asociați
GDPR	Article 28	Both	Supporting	Guvernanța persoanelor împuternicite și instrucțiuni
GDPR	Article 30	Both	Supporting	Evidențe de prelucrare și dovezi privind responsabilitatea
GDPR	Article 37	Conditional	Referenced	Desemnarea DPO acolo unde este aplicabil
GDPR	Article 38	Conditional	Supporting	Poziția și independența DPO acolo unde este aplicabil
GDPR	Article 39	Conditional	Supporting	Sarcinile DPO acolo unde este aplicabil
ISO/IEC 29100:2020	Clause 4.1; Clause 4.2	Both	Supporting	Actori și roluri din cadrul de protecție a confidențialității
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Responsabilitate pentru conformitatea privind confidențialitatea
ISO/IEC 29151:2022	Clause 6.1.2; Clause 6.1.3	Both	Supporting	Roluri de protecție a PII și separare
ISO/IEC 27002:2022	Control 5.2	Both	Supporting	Roluri și responsabilități privind securitatea informației
ISO/IEC 27002:2022	Control 5.3	Both	Supporting	Separarea atribuțiilor

1. Domeniu de aplicare

1.1 Această politică definește modelul de roluri PIMS, structura responsabilității, regulile de atribuire a responsabilităților, regulile de combinare a rolurilor, așteptările privind escaladarea și cerințele privind dovezile pentru guvernanța confidențialității.

1.2 Această politică se aplică personalului, funcțiilor, sistemelor, furnizorilor, persoanelor împuternicite, persoanelor subîmputernicite și relațiilor de operatori asociați care participă la sau influențează prelucrarea PII în domeniul de aplicare al PIMS.

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

1.4 Această politică nu creează noi denumiri de posturi organizaționale. Aceasta definește roluri PIMS canonice care pot fi atribuite personalului sau funcțiilor existente, cu condiția ca cerințele privind atribuirea rolului, competența, independența și conflictul de interese să fie documentate.

2. Scop

2.1 Scopul acestei politici este de a asigura faptul că responsabilitățile PIMS sunt atribuite clar, înțelese, comunicate, demonstrate prin dovezi, revizuite și îmbunătățite.

2.2 Această politică permite organizației să demonstreze responsabilitatea pentru guvernanța confidențialității, deținerea prelucrării PII, determinarea rolurilor de operator și persoană împuternicită, alocarea responsabilităților între operatori asociați, gestionarea instrucțiunilor pentru persoana împuternicită, responsabilitatea furnizorilor privind confidențialitatea, revizuirea independentă și escaladarea bazată pe roluri.

3. Obiective

3.1 Obiectivele acestei politici sunt de a:

3.1.1 defini rolurile PIMS canonice utilizate în întregul set de politici PIMS;

3.1.2 asigura că fiecare responsabilitate PIMS semnificativă are un rol responsabil atribuit;

3.1.3 susține responsabilitatea în calitate de operator, operator asociat, persoană împuternicită și persoană subîmputernicită;

3.1.4 permite combinarea practică a rolurilor pentru organizațiile mici și mijlocii, controlând în același timp conflictele de interese;

3.1.5 păstra revizuirea independentă de către Internal Audit / Compliance Reviewer;

3.1.6 asigura că atribuirile de roluri și schimbările de roluri sunt înregistrate în obiectele de dovezi canonice;

3.1.7 asigura că deținătorii de roluri PIMS primesc comunicarea și conștientizarea adecvate;

3.1.8 asigura că lacunele, conflictele și neconformitățile legate de roluri sunt escaladate și corectate.

4. Declarații de politică

4.1 Modelul de roluri PIMS și atribuirea rolurilor

4.1.1 [All] Top Management TREBUIE să aprobe modelul de roluri PIMS canonic în REG01 înainte de implementarea inițială a PIMS și anual ulterior.

4.1.2 [All] Privacy Lead / PIMS Manager TREBUIE să mențină atribuirile nominale de roluri PIMS în REG01 înainte de implementarea PIMS și în termen de 10 zile lucrătoare de la schimbările de personal sau organizaționale.

4.1.3 [All] Privacy Lead / PIMS Manager TREBUIE să documenteze domeniul responsabilității și nivelul de autoritate pentru fiecare rol PIMS atribuit în REG01 înainte ca atribuirea să intre în vigoare.

4.1.4 [All] Process Owner / Business Owner TREBUIE să atribuie un proprietar responsabil pentru prelucrare pentru fiecare activitate de prelucrare PII în REG02 înainte de începerea activității de prelucrare.

4.1.5 [All] System Owner / Application Owner TREBUIE să documenteze proprietarul de sistem responsabil pentru fiecare sistem care prelucrează PII în REG02 înainte de intrarea sistemului în producție.

4.1.6 [All] Vendor / Procurement Owner TREBUIE să documenteze proprietarul relației pentru fiecare persoană împuternicită, persoană subîmputernicită, partajare de date cu terți sau relație de operatori asociați în REG08 înainte de integrare sau de aprobarea acordului.

4.2 Combinarea rolurilor, separarea și independența

4.2.1 [All] Privacy Lead / PIMS Manager TREBUIE să documenteze fiecare combinare a rolurilor PIMS în REG01 înainte ca acea combinare a rolurilor să intre în vigoare.

4.2.2 [All] Top Management TREBUIE să aprobe în REG01, înainte de atribuire, combinările de roluri care implică Privacy Lead / PIMS Manager, Data Protection Officer / Privacy Advisor, Information Security Lead, Incident Response Coordinator sau Internal Audit / Compliance Reviewer.

4.2.3 [All] Internal Audit / Compliance Reviewer TREBUIE să documenteze independența față de procesul PIMS supus revizuirii în REG12 înainte de începerea fiecărui audit PIMS sau a fiecărei revizuiri de conformitate.

4.2.4 [All] Privacy Lead / PIMS Manager TREBUIE să înregistreze controalele compensatorii pentru conflictele inevitabile privind separarea atribuțiilor în REG12 înainte de aprobarea unei combinări de roluri.

4.2.5 [All] Data Protection Officer / Privacy Advisor TREBUIE să înregistreze preocupările privind independența rolului sau preocupările privind conflictul de interese în REG12 în termen de cinci zile lucrătoare de la identificare.

[... 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 solicite o excepție privind responsabilitatea pe roluri în REG12 înainte de operarea unei activități de prelucrare PII fără un rol atribuit obligatoriu.

9.1.2 [All] Privacy Lead / PIMS Manager TREBUIE să evalueze impactul și măsurile de atenuare pentru fiecare excepție privind responsabilitatea pe roluri în REG12 în termen de 10 zile lucrătoare de la solicitare.

9.1.3 [All] Top Management TREBUIE să aprobe excepțiile privind responsabilitatea pe roluri care depășesc 30 de zile sau afectează prelucrări cu risc ridicat în REG12 înainte ca excepția să intre în vigoare.

9.1.4 [All] Privacy Lead / PIMS Manager TREBUIE să stabilească în REG12 o dată de expirare care nu depășește 90 de zile pentru fiecare excepție aprobată privind responsabilitatea pe roluri înainte de aprobare.

9.1.5 [All] Privacy Lead / PIMS Manager TREBUIE să închidă sau să reevalueze fiecare excepție privind responsabilitatea pe roluri în REG12 în termen de cinci zile lucrătoare de la expirare.

10. Aplicare

10.1.1 [All] Privacy Lead / PIMS Manager TREBUIE să înregistreze atribuirile de roluri PIMS lipsă, inexacte sau depășite ca neconformități în REG12 în termen de cinci zile lucrătoare de la identificare.

10.1.2 [All] Top Management TREBUIE să solicite acțiuni corective în REG12 în termen de 15 zile lucrătoare pentru eșecuri repetate sau prelungite ale responsabilității.

10.1.3 [All] Process Owner / Business Owner TREBUIE să împiedice intrarea în producție a prelucrărilor PII noi sau modificate atunci când dovezile obligatorii privind rolurile și responsabilitatea lipsesc din REG02 sau REG08.

10.1.4 [All] Internal Audit / Compliance Reviewer TREBUIE să verifice eficacitatea acțiunilor corective pentru neconformitățile privind responsabilitatea pe roluri în REG12 la următorul audit programat sau în termen de 60 de zile de la închidere, oricare dintre acestea survine prima.

11. Revizuire și întreținere

11.1.1 [All] Privacy Lead / PIMS Manager TREBUIE să revizuiască această politică anual și în termen de 30 de zile de la o schimbare semnificativă a modelului de roluri PIMS.

11.1.2 [All] Data Protection Officer / Privacy Advisor TREBUIE să revizuiască modificările propuse ale acestei politici din perspectiva impactului asupra rolurilor privind confidențialitatea în REG12 înainte de aprobare.

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

11.1.4 [All] Privacy Lead / PIMS Manager TREBUIE să actualizeze REG01 și REG11 în termen de 15 zile lucrătoare după modificările aprobate ale rolurilor, responsabilităților sau cerințelor de comunicare PIMS.

12. Politici conexe

12.1 Această politică este susținută de următoarele politici conexe:

12.2 PII01 - Politica privind Sistemul de management al informațiilor privind confidențialitatea

12.3 PII03 - Politica privind inventarul prelucrărilor PII și temeiul legal

12.4 PII07 - Politica privind evaluarea riscurilor privind confidențialitatea și DPIA

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

12.6 PII12 - Politica privind managementul confidențialității pentru persoane împuternicite, persoane subîmputernicite și terți

12.7 PII14 - Politica privind securitatea PII și controlul accesului

12.8 PII15 - Politica privind incidentele și încălcările referitoare la PII

12.9 PII16 - Politica privind instruirea, conștientizarea și competența în domeniul confidențialității

12.10 PII17 - Politica privind informațiile documentate și gestionarea dovezilor PIMS

12.11 PII18 - Politica privind monitorizarea, auditul și îmbunătățirea PIMS

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 susțin.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 4.1** - Mapată la determinarea contextului rolurilor PIMS, aplicabilitatea pentru operator și persoană împuternicită, deținerea prelucrării și înregistrările privind responsabilitatea relațiilor. Addressed by clauses [4.3.5; 5.1.5; 5.1.7; 7.1.2].

13.2.2 **Clause 5.1** - Mapată la aprobarea de către Top Management, supravegherea responsabilității, revizuirea anuală de management, metricile de responsabilitate și acțiunile corective pentru eșecurile legate de roluri. Addressed by clauses [4.1.1; 4.2.2; 5.1.1; 6.1.1; 8.1.6; 10.1.2; 11.1.3].

13.2.3 **Clause 5.3** - Mapată la atribuirea, documentarea, comunicarea și menținerea rolurilor, responsabilităților și autorităților PIMS, deținerea sistemelor, deținerea prelucrării, deținerea relațiilor cu furnizorii, deținerea escaladării incidentelor și responsabilitatea pentru revizuire independentă. Addressed by clauses [4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.4.2; 4.4.3; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.4 **Clause 7.2** - Mapată la dovezile privind competența și conștientizarea specifice rolului pentru responsabilitățile PIMS atribuite. Addressed by clauses [7.1.4; 8.1.5].

13.2.5 **Clause 7.3** - Mapată la conștientizarea responsabilităților PIMS atribuite, dovezile de confirmare și raportarea anuală a conștientizării rolurilor. Addressed by clauses [4.5.1; 4.5.2; 7.1.4; 8.1.5].

13.2.6 **Clause 7.4** - Mapată la comunicarea atribuirilor de roluri, a schimbărilor de roluri, a escaladărilor și a informațiilor de predare a rolurilor. Addressed by clauses [4.5.1; 4.5.4; 6.1.5; 7.1.6].

13.2.7 **Clause 7.5** - Mapată la informațiile documentate pentru atribuirile de roluri PIMS, domeniile responsabilităților, nivelurile de autoritate, păstrarea anuală a dovezilor și menținerea matricei de roluri. Addressed by clauses [4.1.2; 4.1.3; 4.5.3; 7.1.1; 11.1.4].

13.2.8 **Clause 8.1** - Mapată la deținerea controlului operațional pentru activități de prelucrare, sisteme, furnizori, persoane împuternicite, persoane subîmputernicite, relații de operatori asociați și controale de intrare în producție. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 7.1.2; 7.1.3; 7.1.5; 10.1.3].

13.2.9 **Clause 9.2** - Mapată la auditul independent și la revizuirea de conformitate a dovezilor privind atribuirea rolurilor, a dovezilor privind combinarea rolurilor, a dovezilor privind independența, a constatărilor și a închiderii acțiunilor corective. Addressed by clauses [4.2.3; 5.1.9; 6.1.4; 8.1.4; 10.1.4].

13.2.10 **Clause 9.3** - Mapată la revizuirea de management a caracterului complet al atribuirilor de roluri PIMS, a conflictelor de roluri, a excepțiilor, a metricilor de responsabilitate și a rezultatelor revizuirii responsabilității. Addressed by clauses [5.1.1; 6.1.1; 8.1.6; 11.1.1].

13.2.11 **Clause 10.2** - Mapată la escaladarea, înregistrarea neconformităților, acțiunile corective, închiderea excepțiilor și verificarea eficacității pentru problemele privind responsabilitatea pe roluri. Addressed by clauses [4.2.5; 4.4.5; 6.1.5; 9.1.5; 10.1.1; 10.1.2; 10.1.4].

13.2.12 **Annex A.1.2.7** - Mapată la atribuirea și documentarea responsabilității pentru contractul cu persoana împuternicită și a escaladării responsabilității terților înainte de aprobarea sau reînnoirea contractului. Addressed by clauses [4.1.6; 4.4.4; 5.1.7; 7.1.3].

13.2.13 **Annex A.1.2.8** - Mapată la documentarea alocării responsabilităților între operatori asociați și a dovezilor privind responsabilitatea relației înainte de începerea prelucrării de către operatori asociați. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.2.14 **Annex A.1.2.9** - Mapată la menținerea înregistrărilor de responsabilitate pentru deținerea prelucrării de către operator, clasificarea rolurilor și deținerea dovezilor. Addressed by clauses [4.3.1; 4.3.5; 4.5.3; 8.1.1].

13.2.15 **Annex A.2.2.2** - Mapată la responsabilitatea pentru acordurile cu clienții ale persoanei împuternicite, deținerea instrucțiunilor clientului și dovezile privind relația cu persoana împuternicită. Addressed by clauses [4.3.3; 5.1.7; 7.1.3; 8.1.3].

13.2.16 **Annex A.2.2.3** - Mapată la alinierea scopului și instrucțiunilor persoanei împuternicite prin deținerea instrucțiunilor clientului și verificarea rolurilor de operator/persoană împuternicită. Addressed by clauses [4.3.3; 4.3.5; 5.1.7].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapat la dovezile de responsabilitate pentru atribuirile de roluri, deținerea prelucrării, revizuirile rolurilor, neconformități și constatări de audit. Addressed by clauses [4.5.3; 6.1.2; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Mapat la responsabilitatea operatorului, deținerea responsabilă a prelucrării, supravegherea de către Top Management, revizuirea anuală și măsurile de responsabilitate. Addressed by clauses [4.1.1; 4.3.1; 5.1.1; 6.1.1; 8.1.6].

13.3.3 **Article 26** - Mapat la documentarea alocării responsabilităților între operatori asociați și a dovezilor privind responsabilitatea relației înainte de începerea prelucrării de către operatori asociați. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.3.4 **Article 28** - Mapat la alocarea responsabilităților persoanelor împuternicite și persoanelor subîmputernicite, deținerea instrucțiunilor clientului, responsabilitatea contractuală și căile de escaladare pentru terți. Addressed by clauses [4.3.3; 4.3.4; 4.4.4; 5.1.7; 7.1.3].

13.3.5 **Article 30** - Mapat la evidențele de prelucrare, deținerea prelucrării, clasificarea rolurilor PIMS și verificarea rolurilor de operator/persoană împuternicită. Addressed by clauses [4.1.4; 4.3.1; 4.3.5; 8.1.1].

13.3.6 **Article 37** - Mapat la documentarea rolului Data Protection Officer / Privacy Advisor acolo unde desemnarea este aplicabilă sau este realizată voluntar. Addressed by clauses [4.1.2; 4.1.3; 5.1.3; 11.1.2].

13.3.7 **Article 38** - Mapat la poziția, independența, implicarea și gestionarea conflictelor de interese ale Data Protection Officer / Privacy Advisor acolo unde este aplicabil. Addressed by clauses [4.2.5; 5.1.3; 6.1.3; 11.1.2].

13.3.8 **Article 39** - Mapat la consilierea privind confidențialitatea, observațiile de monitorizare, revizuirea consultativă și revizuirea impactului asupra confidențialității legat de roluri de către Data Protection Officer / Privacy Advisor acolo unde este aplicabil. Addressed by clauses [4.4.1; 5.1.3; 6.1.3; 11.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.1; Clause 4.2** - Mapate la actorii din cadrul de protecție a confidențialității și la alocarea rolurilor pentru PII principals, operatori PII, persoane împuternicite PII, terți și clasificarea rolurilor PIMS. Addressed by clauses [4.1.4; 4.1.6; 4.3.5; 5.1.5; 5.1.7].

13.4.2 **Clause 5.12** - Mapată la responsabilitatea pentru conformitatea privind confidențialitatea, dovezi de rol, revizuire, constatări de audit și verificarea acțiunilor corective. Addressed by clauses [4.5.3; 6.1.2; 8.1.4; 10.1.4].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 6.1.2; Clause 6.1.3** - Mapate la definirea rolurilor de protecție a PII, documentarea rolurilor, comunicarea rolurilor, coordonarea securitate/confidențialitate și separarea atribuțiilor pentru protecția PII. Addressed by clauses [4.1.1; 4.2.1; 4.2.3; 4.2.4; 4.4.2; 5.1.4; 7.1.4].

13.6 ISO/IEC 27002:2022

13.6.1 Control 5.2 - Mapat la definirea, alocarea, documentarea, comunicarea și menținerea responsabilităților PIMS și de securitate a informației. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.2; 4.5.1; 5.1.4; 7.1.1].

13.6.2 Control 5.3 - Mapat la separarea atribuțiilor, aprobarea combinării rolurilor, revizuirea independentă, controalele privind conflictele și verificarea acțiunilor corective pentru conflictele de roluri. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 9.1.2; 10.1.4].