					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: PII14					Titlul documentului: **Politica privind securitatea și controlul accesului pentru PII**							
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 6.1.3; Clause 8.1	Both	Primary	Planificarea și operarea controalelor de securitate pentru PII
ISO/IEC 27701:2025	Clause 7.5; Clause 9.1; Clause 10.2	Both	Supporting	Dovezi, monitorizare și acțiune corectivă
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9	Both	Primary	Identitate și drepturi de acces pentru prelucrarea PII
ISO/IEC 27701:2025	Annex A.3.22; Annex A.3.23	Both	Primary	Protecția punctelor terminale și autentificare securizată
ISO/IEC 27701:2025	Annex A.3.25; Annex A.3.26	Both	Primary	Jurnalizare și protecție criptografică
ISO/IEC 27701:2025	Annex A.3.28; Annex A.3.29	Both	Supporting	Securitatea aplicațiilor și arhitectură securizată
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.15; Annex A.3.16	Both	Supporting	Protecția și revizuirea înregistrărilor
GDPR	Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32	Both	Primary	Securitate, responsabilitate și controale pentru persoanele împuternicite
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Integrarea controalelor SMSI
ISO/IEC 27002:2022	Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Îndrumări pentru implementarea controalelor de securitate
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Principii de securitate a informației și de

				conformitate privind confidențialitatea
ISO/IEC 29151:2022	Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	Controale de securitate pentru protecția PII

1. Domeniu de aplicare

1.1 Prezenta politică definește cerințele de securitate și de control al accesului specifice PII pentru sisteme, aplicații, servicii, dispozitive, medii cloud și procese operaționale care stochează, transmit, prelucrează, accesează, administrează sau protejează PII.

1.2 Prezenta politică se aplică în contexte de operator, operator asociat, persoană împuternicită și persoană subîmputernicită în care organizația determină, operează, susține sau se bazează pe controale de securitate pentru prelucrarea PII.

1.3 Prezenta politică acoperă următoarele domenii de control de securitate pentru PII:

1.3.1 baza de referință pentru securitatea PII și integrarea cu politicile existente de securitate a informației;

1.3.2 controlul accesului;

1.3.3 autentificare;

1.3.4 acces privilegiat;

1.3.5 criptare și stocare securizată;

1.3.6 jurnalizare și monitorizare;

1.3.7 configurare securizată și managementul vulnerabilităților;

1.3.8 controale de acces pentru puncte terminale și cloud;

1.3.9 legarea dovezilor prin REG02, REG08, REG10 și REG12.

1.4 Prezenta politică nu înlocuiește un sistem complet de management al securității informației, o politică de securitate a rețelei, o politică de dezvoltare securizată, o politică de backup, o politică privind punctele terminale, o politică de securitate cloud, un standard criptografic, o procedură de management al vulnerabilităților sau o procedură de răspuns la incidente. În cazul în care aceste politici există deja, prezenta politică definește legătura specifică PII și cerințele de dovezi necesare pentru asigurarea PIMS.

1.5 Prezenta politică nu dublează:

1.5.1 inventarul prelucrărilor PII și deținerea temeiului juridic din PII03;

1.5.2 metodologia pentru evaluarea riscurilor privind confidențialitatea și DPIA din PII07;

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

1.5.4 regulile de colectare, utilizare, divulgare și partajare din PII09;

1.5.5 executarea retenției, ștergerii și eliminării din PII10;

1.5.6 guvernanța ciclului de viață al persoanelor împuternicite din PII12;

1.5.7 controalele mecanismelor de transfer internațional din PII13;

1.5.8 fluxul de lucru pentru incidente și încălcări din PII15;

1.5.9 guvernanța informațiilor documentate din PII17;

1.5.10 guvernanța monitorizării, auditului și îmbunătățirii PIMS din PII18.

1.6 Pentru prezenta politică, jurnalele operaționale, rezultatele instrumentelor de securitate, exporturile revizuirilor accesului, rapoartele de vulnerabilitate și dovezile de configurare sunt surse de dovezi care sunt atașate la, rezumate în sau referențiate de obiectele canonice de dovezi. Acestea nu constituie registre PIMS separate.

2. Scop

2.1 Scopul prezentei politici este de a asigura că PII sunt protejate prin controale de securitate și de acces adecvate, aliniate la risc și auditabile pe parcursul prelucrării.

2.2 Prezenta politică permite organizației să demonstreze că controalele de securitate pentru PII sunt planificate, implementate, revizuite, monitorizate și îmbunătățite prin REG02, REG08, REG10 și

REG12, fără a crea registre de securitate duplicate și fără a înlocui politicile existente de securitate a informației.

3. Obiective

3.1 Obiectivele prezentei politici sunt următoarele:

3.1.1 să definească o bază de referință pentru controlul accesului la PII pentru sisteme și activități de prelucrare;

3.1.2 să asigure că mecanismele de autentificare sunt adecvate sensibilității PII și contextului de acces;

3.1.3 să definească cerințe de revizuire pentru accesul privilegiat și accesul obișnuit la PII;

3.1.4 să definească așteptările privind criptarea și stocarea securizată pentru PII în repaus, în tranzit și în contexte relevante cloud sau ale punctelor terminale;

3.1.5 să definească așteptările privind jurnalizarea și monitorizarea accesului la PII, modificărilor asupra PII și administrării PII;

3.1.6 să definească cerințele de dovezi privind configurarea securizată și vulnerabilitățile pentru sistemele care prelucrează PII;

3.1.7 să definească așteptările privind accesul de pe puncte terminale și din cloud, fără a crea o politică completă privind punctele terminale sau securitatea cloud;

3.1.8 să lege incidentele de securitate PII suspectate de REG10, fără a duplica fluxul de lucru pentru incidente;

3.1.9 să se integreze cu politicile existente de securitate a informației, acolo unde acestea sunt disponibile;

3.1.10 să mențină dovezi pregătite pentru audit utilizând exclusiv REG02, REG08, REG10 și REG12.

4. Declarații de politică

4.1 Baza de referință pentru securitatea PII și integrarea cu SMSI

4.1.1 [Both] Information Security Lead trebuie să definească baza de referință pentru securitatea PII pentru fiecare sistem sau serviciu care prelucrează PII în REG12 înainte ca sistemul sau serviciul să intre în producție sau să fie modificat semnificativ.

4.1.2 [Both] System Owner / Application Owner trebuie să înregistreze în REG12 locația dovezilor privind controalele de securitate PII implementate înainte de a se baza pe un control existent de securitate a informației pentru asigurarea PIMS.

4.1.3 [Controller] Process Owner / Business Owner trebuie să identifice sensibilitatea PII, contextul prelucrării și nevoia de acces în REG02 înainte de a solicita acces nou sau modificat semnificativ la PII.

4.1.4 [Processor] Vendor / Procurement Owner trebuie să înregistreze în REG08 instrucțiunile de securitate ale clientului, limitele responsabilităților clientului și angajamentele de securitate ale persoanei împuternicite înainte ca accesul persoanei împuternicite la PII ale clientului să înceapă sau să fie modificat semnificativ.

4.1.5 [Both] Privacy Lead / PIMS Manager trebuie să verifice că dovezile de securitate pentru PII sunt legate de REG02, REG08, REG10 sau REG12 înainte de a accepta activitatea de prelucrare ca fiind auditabilă în cadrul PIMS.

4.2 Baza de referință pentru controlul accesului

4.2.1 [Both] System Owner / Application Owner trebuie să restricționeze accesul la PII la rolurile aprobate și utilizatorii autorizați înregistrați sau trasabili în REG02 sau REG12 înainte ca accesul să fie activat.

4.2.2 [Both] Process Owner / Business Owner trebuie să aprobe scopul operațional pentru accesul la PII în REG02 sau REG12 înainte ca System Owner / Application Owner să aloce accesul.

4.2.3 [Both] System Owner / Application Owner trebuie să revizuiască accesul utilizatorilor la sistemele care prelucrează PII cu impact ridicat sau sensibile cel puțin trimestrial și să înregistreze rezultatul revizuirii în REG12.

4.2.4 [Both] System Owner / Application Owner trebuie să revizuiască accesul utilizatorilor la alte sisteme care prelucrează PII cel puțin anual și să înregistreze rezultatul revizuirii în REG12.

4.2.5 [Both] System Owner / Application Owner trebuie să elimine sau să modifice accesul la PII în REG12 în termen de o zi lucrătoare după schimbarea rolului, încetarea raportului, finalizarea contractului sau momentul în care accesul nu mai este necesar.

4.2.6 [Processor] Vendor / Procurement Owner trebuie să confirme în REG08 că accesul persoanei împuternicite la PII ale clientului este limitat la instrucțiunile documentate ale clientului înainte ca accesul să fie activat sau modificat.

4.2.7 [Subprocessor] Vendor / Procurement Owner trebuie să confirme în REG08 că accesul persoanei subîmputernicite la PII este limitat la activitățile de subîmputernicire autorizate înainte ca accesul persoanei subîmputernicite să fie activat sau modificat.

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

9. Excepții

9.1.1 [Both] Information Security Lead trebuie să înregistreze fiecare excepție de la o cerință de securitate PII sau de control al accesului în REG12 înainte ca excepția să fie activată.

9.1.2 [Both] Data Protection Officer / Privacy Advisor trebuie să ofere consultanță privind excepțiile de securitate PII cu risc mai ridicat în REG12 înainte de aprobare.

9.1.3 [Both] Top Management trebuie să aprobe excepțiile de securitate PII în REG12 înainte de activare atunci când excepția afectează PII cu impact ridicat, PII sensibile, acces privilegiat, criptare, jurnalizare sau vulnerabilități nerezolvate cu risc ridicat.

9.1.4 [Both] Information Security Lead trebuie să definească în REG12 data de expirare a excepției, controlul compensatoriu și data revizuirii înainte de aprobarea excepției.

9.1.5 [Both] System Owner / Application Owner trebuie să remedieze, să reînnoiască sau să închidă excepțiile de securitate PII expirate în REG12 în termen de cinci zile lucrătoare după expirare.

9.1.6 [Processor] Vendor / Procurement Owner trebuie să înregistreze în REG08 și REG12 excepțiile de securitate ale persoanelor împuternicite sau persoanelor subîmputernicite care afectează PII ale clientului înainte de acceptare.

10. Aplicare

10.1.1 [Both] Privacy Lead / PIMS Manager trebuie să înregistreze în REG12 neconformitățile pentru dovezile de securitate PII lipsă sau incomplete în termen de cinci zile lucrătoare de la identificare.

10.1.2 [Both] Information Security Lead trebuie să atribuie responsabilitatea remedierii eșecurilor controalelor de securitate PII în REG12 în termen de cinci zile lucrătoare de la validare.

10.1.3 [Both] System Owner / Application Owner trebuie să dezactiveze sau să restricționeze accesul la PII neautorizat, excesiv sau nesusținut în termen de o zi lucrătoare de la validare și să înregistreze acțiunea în REG12.

10.1.4 [Conditional] Incident Response Coordinator trebuie să lege măsurile de aplicare de REG10 în termen de o zi lucrătoare atunci când aspectul supus aplicării implică un incident PII suspectat sau confirmat.

10.1.5 [Both] Top Management trebuie să revizuiască neconformitățile de securitate PII repetate sau cu risc ridicat în REG12 înainte de revizuirea de management.

11. Revizuire și mentenanță

11.1.1 [All] Privacy Lead / PIMS Manager trebuie să revizuiască prezenta politică împreună cu Information Security Lead cel puțin anual și să înregistreze rezultatul revizuirii în REG12.

11.1.2 [Both] Information Security Lead trebuie să revizuiască baza de referință pentru securitatea PII în REG12 în termen de 30 de zile după o modificare semnificativă de tehnologie, amenințare, audit, incident sau reglementare care afectează securitatea PII.

11.1.3 [Both] System Owner / Application Owner trebuie să actualizeze dovezile de securitate PII la nivel de sistem în REG12 în termen de 30 de zile după o modificare semnificativă de arhitectură, acces, configurare, vulnerabilitate sau jurnalizare.

11.1.4 [Processor] Vendor / Procurement Owner trebuie să revizuiască dovezile privind responsabilitățile de securitate PII ale persoanelor împuternicite și persoanelor subîmputernicite în REG08 în termen de 30 de zile după o modificare semnificativă a serviciului, a instrucțiunilor clientului sau a persoanei subîmputernicite.

11.1.5 [All] Internal Audit / Compliance Reviewer trebuie să verifice dovezile de revizuire a politicii și dovezile selectate privind controalele de securitate PII în REG12 conform planului de audit aprobat.

12. Politici conexe

12.1 Prezenta politică trebuie citită împreună cu:

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

12.1.2 PII02 - Politica privind rolurile, responsabilitățile și responsabilitatea în materie de confidențialitate;

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

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

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

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

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

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

12.1.9 PII13 - Politica privind transferul internațional al PII;

12.1.10 PII15 - Politica de management al incidentelor și încălcărilor PII;

12.1.11 PII16 - Politica privind instruirea, conștientizarea și competența în materie de confidențialitate;

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

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

13. Standarde și cadre de referință

13.1 ISO/IEC 27701:2025 - Clause 6.1.3; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.7; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5; 5.1.4; 5.1.6; 6.1.2; 7.1.1; 7.1.2].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.5.5; 4.6.3; 4.6.4; 4.7.5; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 7.1.3; 7.1.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.2; 11.1.1; 11.1.5].

13.3 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 10.1.3].

13.4 ISO/IEC 27701:2025 - Annex A.3.22; Annex A.3.23. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5].

13.5 ISO/IEC 27701:2025 - Annex A.3.25; Annex A.3.26. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.6 ISO/IEC 27701:2025 - Annex A.3.28; Annex A.3.29. Addressed by clauses [4.1.1; 4.1.2; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 7.1.1; 7.1.2].

13.7 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.15; Annex A.3.16. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.6.2; 4.6.3; 4.6.4; 4.7.2; 4.7.3; 5.1.9; 6.1.6; 8.1.4; 10.1.1; 11.1.5].

13.8 GDPR - Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.5; 4.2.6; 4.2.7; 4.3.2; 4.4.4; 4.5.1; 4.5.2; 4.6.1; 4.6.6; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 4.8.5; 5.1.1; 5.1.7; 6.1.4; 7.1.4; 9.1.3; 10.1.4].

13.9 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.10 ISO/IEC 27002:2022 - Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.11 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.1; 4.5.1; 4.6.2; 4.6.6; 4.7.6; 5.1.2; 6.1.1; 8.1.4; 10.1.1; 11.1.1].

13.12 ISO/IEC 29151:2022 - Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.7.1; 4.7.2; 4.7.4; 4.8.1; 4.8.2; 6.1.6; 11.1.5].