					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: PII15-FS					Titlul documentului: **Politica de gestionare a incidentelor și încălcărilor privind PII în sectorul financiar**							
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 / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Comunicări PIMS și dovezi documentate privind incidentele
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Control operațional, evaluarea riscurilor privind confidențialitatea și legătura cu tratamentul riscurilor
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorizare, evaluare, neconformitate, acțiune corectivă și îmbunătățire
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Planificarea și pregătirea gestionării incidentelor pentru prelucrarea PII
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Răspuns la incidente de securitate a informațiilor care implică PII
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Cerințe legale, statutare, de reglementare și contractuale, precum și protecția înregistrărilor
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Acordul cu clientul persoanei împuternicite și suport pentru obligațiile clientului
GDPR	Article 5(2); Article 24	Controller	Supporting	Responsabilitate și răspunderea operatorului
GDPR	Article 26	Joint Controller	Supporting	Coordonarea responsabilităților operatorilor asociați privind incidentele

GDPR	Article 28	Both	Supporting	Asistența persoanei împuternicite și obligații contractuale ale persoanei împuternicite
GDPR	Article 32	Both	Supporting	Securitatea prelucrării și capacitatea de detectare a încălcărilor
GDPR	Article 33	Both	Primary	Notificarea încălcării securității datelor cu caracter personal și documentarea încălcării
GDPR	Article 34	Controller	Primary	Comunicarea încălcărilor securității datelor cu caracter personal către persoanele vizate afectate
GDPR	Article 39	Conditional	Supporting	Consiliere din partea DPO, monitorizare, cooperare și suport ca punct de contact
DORA Regulation (EU) 2022/2554	Article 17	Conditional	Primary	Proces de gestionare a incidentelor legate de ICT pentru entitățile financiare incluse în domeniul de aplicare
DORA Regulation (EU) 2022/2554	Article 18	Conditional	Primary	Criterii de clasificare a incidentelor legate de ICT și a amenințărilor cibernetice semnificative
DORA Regulation (EU) 2022/2554	Article 19	Conditional	Primary	Raportarea incidentelor majore legate de ICT și notificarea amenințărilor

				cibernetice semnificative
DORA Regulation (EU) 2022/2554	Article 20	Conditional	Supporting	Conținutul raportării, termene, modele și proceduri
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Raportarea incidentelor semnificative, după caz
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Principii de securitate a informațiilor și conformitate privind confidențialitatea
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Responsabilități de răspuns la incidente PII și raportarea evenimentelor
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Planificarea, evaluarea, răspunsul, lecțiile învățate și colectarea dovezilor privind incidentele
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Ciclul de viață al procesului de gestionare a incidentelor
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Politica, planul, conștientizarea, testarea și lecțiile învățate privind incidentele
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Operațiuni de detectare, notificare, triaj, analiză, răspuns și raportare
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Așteptări privind notificarea și înregistrarea încălcărilor pentru persoanele împuternicite din cloud public

1. Domeniu de aplicare

1.1 Această politică definește cerințele pentru identificarea, raportarea, trierea, clasificarea, evaluarea, conținerea, notificarea, documentarea, închiderea și îmbunătățirea pe baza incidentelor PII și a încălcărilor PII în domeniile de aplicare PIMS din sectorul financiar.

1.2 **Notă de implementare:** Această politică este o variantă de înlocuire pentru sectorul financiar a PII15. Ea nu trebuie implementată simultan cu PII15 pentru același domeniu de aplicare PIMS, aceeași unitate de business, același produs, mediu de client, serviciu reglementat sau perimetru al dovezilor. Organizațiile trebuie să selecteze fie PII15, fie PII15-FS pentru același domeniu de aplicare, pentru a evita obligații duplicate de gestionare a incidentelor, registre duplicate și activități duplicate privind dovezile de audit.

1.3 Această politică se aplică:

1.3.1 organizației care acționează ca operator PII într-un context de sector financiar;

1.3.2 organizației care acționează ca operator asociat atunci când este necesară coordonarea responsabilităților privind incidentele sau încălcările;

1.3.3 organizației care acționează ca persoană împuternicită PII pentru clienți din sectorul financiar;

1.3.4 organizației care acționează ca persoană subîmputernicită pentru clienți din sectorul financiar sau pentru persoane împuternicite din amonte;

1.3.5 sistemelor, aplicațiilor, serviciilor, proceselor, furnizorilor, persoanelor împuternicite, persoanelor subîmputernicite și terților care prelucrează, stochează, transmit, susțin, accesează sau afectează în alt mod PII în cadrul domeniului de aplicare PIMS din sectorul financiar.

1.4 Această politică utilizează REG10 - Registrul incidentelor și încălcărilor privind PII ca obiect principal de dovezi pentru gestionarea incidentelor și încălcărilor privind PII în sectorul financiar.

1.5 Această politică utilizează obiecte-suport de dovezi după cum urmează:

1.5.1 REG01 pentru domeniul de aplicare PIMS și contextul aplicabil al părților interesate, sectorial, al clienților, contractual și de raportare.

1.5.2 REG02 pentru activitățile de prelucrare afectate, categoriile de PII, categoriile de persoane vizate, scopurile, sistemele și serviciile.

1.5.3 REG03 pentru Declarație de aplicabilitate și actualizări privind aplicabilitatea controalelor, inclusiv înlocuirea PII15 cu PII15-FS pentru același domeniu de aplicare.

1.5.4 REG04 pentru legătura cu riscul privind confidențialitatea, DPIA, riscul rezidual și tratamentul riscului.

1.5.5 REG08 pentru dovezi privind interfața de incident cu persoanele împuternicite, persoanele subîmputernicite, clienții, furnizorii și terții.

1.5.6 REG09 pentru legătura cu transferurile internaționale atunci când un incident afectează prelucrarea transfrontalieră.

1.5.7 REG11 pentru dovezi privind instruirea, conștientizarea și competența de răspuns la incidente.

1.5.8 REG12 pentru dovezi privind auditul, neconformitatea, acțiunea corectivă, revizuirea de management și îmbunătățirea.

1.6 Această politică se bazează pe politicile PIMS conexe pentru controale specializate:

1.6.1 PII03 guvernează inventarul prelucrărilor și înregistrările privind temeiul juridic.

1.6.2 PII04 guvernează nota de informare privind confidențialitatea și controalele de transparență din afara comunicărilor specifice încălcărilor.

1.6.3 PII06 guvernează cererile persoanelor vizate privind drepturile care apar înainte, în timpul sau după un incident.

1.6.4 PII07 guvernează metodologia de evaluare a riscurilor privind confidențialitatea și DPIA.

1.6.5 PII08 guvernează controalele privind protecția datelor încă din faza de proiectare și în mod implicit.

1.6.6 PII10 guvernează controalele de păstrare, ștergere și eliminare.

1.6.7 PII12 guvernează controalele relațiilor privind confidențialitatea cu persoanele împuternicite, persoanele subîmputernicite, furnizorii și terții.

1.6.8 PII13 guvernează mecanismele de transfer internațional al PII și înregistrările privind riscul de transfer.

1.6.9 PII14 guvernează controalele preventive și de detectare privind securitatea PII și accesul.

1.6.10 PII16 guvernează instruirea, conștientizarea și competența privind confidențialitatea.

1.6.11 PII17 guvernează informațiile documentate și gestionarea dovezilor.

1.6.12 PII18 guvernează monitorizarea, auditul intern, revizuirea de management, neconformitatea, acțiunea corectivă și îmbunătățirea continuă.

1.6.13 PII23 guvernează controalele persoanei împuternicite PII în cloud atunci când obligațiile persoanei împuternicite din cloud sunt incluse în domeniul de aplicare.

1.7 În sensul acestei politici:

1.7.1 „Incident PII” înseamnă un eveniment suspectat sau confirmat care a afectat, ar fi putut afecta sau ar putea afecta în mod rezonabil confidențialitatea, integritatea, disponibilitatea, prelucrarea legală sau gestionarea autorizată a PII.

1.7.2 „Încălcare PII” înseamnă un incident PII confirmat care implică distrugerea, pierderea, modificarea, divulgarea, accesul, indisponibilitatea sau compromiterea PII în mod neautorizat, ilegal, accidental sau neintenționat.

1.7.3 „Incident PII din sectorul financiar” înseamnă un incident PII care afectează, poate afecta sau este conectat în mod rezonabil cu servicii financiare reglementate, clienți din sectorul financiar, contrapărți financiare, tranzacții financiare, operațiuni financiare sau prelucrarea PII în sectorul financiar.

1.7.4 „Incident major din sectorul financiar” înseamnă un incident PII din sectorul financiar sau un incident ICT conex care îndeplinește criteriile documentate de materialitate sau raportare din REG10.

1.7.5 „Amenințare cibernetică semnificativă” înseamnă o amenințare cibernetică înregistrată în REG10 care ar putea afecta în mod semnificativ serviciile din sectorul financiar incluse în domeniul de aplicare, prelucrarea PII, clienții, contrapărțile sau operațiunile.

1.7.6 „Evaluarea încălcării securității datelor” înseamnă evaluarea documentată a măsurii în care un incident PII este o încălcare PII, a PII și persoanelor vizate afectate, a riscurilor care pot apărea, a notificărilor sau comunicărilor necesare și a acțiunilor de remediere necesare.

1.7.7 „Conștientizare” înseamnă momentul în care organizația are un grad rezonabil de certitudine că a avut loc un incident de securitate sau de confidențialitate și că PII au fost sau ar fi putut fi compromise.

1.7.8 „Incident PII cu impact ridicat în sectorul financiar” înseamnă un incident PII care implică prelucrări cu risc ridicat, categorii speciale sau PII foarte sensibile, PII la scară largă, persoane vulnerabile, clienți reglementați, perturbări semnificative ale serviciilor, contrapărți financiare, tranzacții financiare, impact în mai multe jurisdicții, compromiterea accesului privilegiat, expunere publică, ransomware, indisponibilitatea serviciilor sau impact operațional, asupra clienților, financiar ori reputațional semnificativ.

1.7.9 „Modificare semnificativă a incidentului” înseamnă informații noi sau modificate care afectează domeniul incidentului, severitatea, categoriile de PII, impactul asupra persoanelor vizate, impactul asupra serviciilor, clasificarea pentru sectorul financiar, decizia de notificare, impactul asupra clienților, cauza principală, conținerea, recuperarea, acțiunea corectivă sau obligațiile de raportare externă.

2. Scop

2.1 Scopul acestei politici este să asigure că incidentele și încălcările privind PII în contexte din sectorul financiar sunt gestionate consecvent, prompt, legal, securizat și cu dovezi pregătite pentru audit.

2.2 Această politică susține responsabilitatea prin impunerea înregistrării incidentelor și încălcărilor privind PII din sectorul financiar în REG10 și corelarea acestora cu înregistrările de prelucrare afectate, riscurile privind confidențialitatea, relațiile cu persoanele împuternicite și persoanele subîmputernicite, înregistrările de transfer, acțiunile corective, înregistrările de instruire, deciziile de raportare în sectorul financiar și dovezile de revizuire de management, atunci când sunt declanșate.

2.3 Această politică asigură că obligațiile operatorului, operatorului asociat, persoanei împuternicite și persoanei subîmputernicite sunt gestionate prin reguli de aplicabilitate distincte, menținând totodată un model integrat de dovezi privind incidentele și încălcările din sectorul financiar.

3. Obiective

3.1 Obiectivele acestei politici sunt:

3.1.1 să asigure raportarea și înregistrarea promptă a incidentelor PII suspectate din sectorul financiar;

3.1.2 să asigure trierea și clasificarea incidentelor PII din sectorul financiar pe baza unor criterii consecvente privind confidențialitatea, securitatea, operațiunile și sectorul;

3.1.3 să asigure că evaluările încălcărilor iau în considerare PII afectate, persoanele vizate, sistemele, serviciile, activitățile de prelucrare, persoanele împuternicite, persoanele subîmputernicite, transferurile, riscurile, clienții, contrapărțile și acțiunile de remediere;

3.1.4 să asigure documentarea deciziilor de notificare ale operatorului și a deciziilor de comunicare către persoanele vizate;

3.1.5 să asigure că notificările privind încălcările transmise de persoanele împuternicite și persoanele subîmputernicite către clienți sau părți din amonte sunt efectuate fără întârzieri nejustificate și în conformitate cu acordurile aplicabile;

3.1.6 să asigure evaluarea, documentarea și urmărirea declanșatorilor de raportare în sectorul financiar, după caz;

3.1.7 să asigure păstrarea și protejarea dovezilor în timpul gestionării incidentelor;

3.1.8 să asigure urmărirea conținerii, eradicării, recuperării și validării prin REG10;

3.1.9 să asigure direcționarea amenințărilor cibernetice semnificative și a incidentelor majore din sectorul financiar către fluxurile adecvate de decizie și raportare;

3.1.10 să asigure că lecțiile învățate din incidente conduc la acțiuni corective, instruire, îmbunătățirea controalelor și revizuire de management;

3.1.11 să asigure disponibilitatea înregistrărilor privind incidentele și încălcările pentru audit, revizuire de management, asigurarea solicitată de clienți și revizuire reglementară, după caz;

3.1.12 să asigure că PII15-FS înlocuiește PII15 pentru același domeniu de aplicare din sectorul financiar și nu dublează activitățile privind dovezile PII15.

4. Declarații de politică

4.1 Activarea variantei, pregătirea și primirea raportărilor

4.1.1 [Conditional] Privacy Lead / PIMS Manager TREBUIE să documenteze activarea PII15-FS în REG01 și REG03 înainte ca această politică să fie utilizată pentru un domeniu de aplicare PIMS din sectorul financiar.

4.1.2 [Conditional] Privacy Lead / PIMS Manager TREBUIE să documenteze în REG03 și REG12 că PII15 nu este implementată simultan pentru același domeniu de aplicare PIMS din sectorul financiar înainte ca PII15-FS să fie aprobată.

4.1.3 [All] Incident Response Coordinator TREBUIE să înregistreze fiecare incident PII suspectat din sectorul financiar, raportat sau detectat, în REG10 în termen de o zi lucrătoare de la primire sau mai devreme atunci când poate fi declanșat un termen aplicabil de notificare, comunicare cu clientul sau raportare.

4.1.4 [Conditional] Privacy Lead / PIMS Manager TREBUIE să mențină criteriile de gestionare a incidentelor și încălcărilor privind PII în sectorul financiar în REG10 cel puțin anual și după orice modificare semnificativă a domeniului de aplicare PIMS, a contextului legal, a obligațiilor față de clienți, a obligațiilor contractuale, a contextului de raportare sectorială sau a prelucrărilor cu risc ridicat.

4.1.5 [Both] Information Security Lead TREBUIE să confirme cerințele de păstrare a dovezilor privind incidentele în REG10 în termen de 24 de ore după ce un incident suspectat afectează un sistem, serviciu sau aplicație care prelucrează PII.

4.1.6 [Conditional] Vendor / Procurement Owner TREBUIE să mențină cerințele privind contactele pentru incidente ale terților din sectorul financiar și rutarea dovezilor în REG08 înainte de integrare și cel puțin anual pentru persoanele împuternicite, persoanele subîmputernicite, furnizorii și prestatorii externalizați de raportare incluși în domeniul de aplicare.

4.2 Clasificare și evaluarea încălcării

4.2.1 [All] Incident Response Coordinator TREBUIE să clasifice fiecare înregistrare REG10 în termen de 24 de ore de la primire ca eveniment non-PII, incident PII suspectat, incident PII confirmat, încălcare PII confirmată, incident PII din sectorul financiar, incident major din sectorul financiar, amenințare cibernetică semnificativă sau înregistrare în curs de clasificare.

4.2.2 [Conditional] Information Security Lead TREBUIE să evalueze serviciile afectate, clienții, contrapărțile, tranzacțiile, timpul de indisponibilitate a serviciilor, răspândirea geografică, pierderea de date, criticitatea serviciilor și impactul economic în REG10 atunci când un incident PII poate afecta servicii sau operațiuni din sectorul financiar.

4.2.3 [Both] Privacy Lead / PIMS Manager TREBUIE să identifice activitatea de prelucrare afectată, categoriile de PII, categoriile de persoane vizate, sistemele, persoanele împuternicite, persoanele subîmputernicite, locațiile de transfer și riscurile privind confidențialitatea în REG02, REG04, REG08, REG09 și REG10 înainte de finalizarea deciziei de notificare a încălcării.

4.2.4 [Controller] Data Protection Officer / Privacy Advisor TREBUIE să evalueze riscul pentru persoanele vizate afectate pentru fiecare încălcare PII confirmată sau suspectată în mod rezonabil și să înregistreze recomandarea de notificare, justificarea riscului și consilierea în REG10 înainte de luarea deciziei de notificare externă.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager TREBUIE să înregistreze alocarea responsabilităților operatorilor asociați privind incidentul în REG08 și REG10 în termen de 24 de ore după identificarea responsabilității partajate pentru o încălcare PII suspectată sau confirmată.

4.2.6 [Processor] Privacy Lead / PIMS Manager TREBUIE să evalueze instrucțiunile clientului, obligațiile contractuale de notificare și obligațiile de cooperare în REG08 și REG10 în termen

de 24 de ore după ce o încălcare PII suspectată sau confirmată afectează prelucrarea efectuată ca persoană împuternicită.

4.2.7 [Subprocessor] Vendor / Procurement Owner TREBUIE să identifice lanțul de notificare din amonte și rutarea necesară a dovezilor în REG08 și REG10 în termen de 24 de ore după ce un incident PII suspectat sau confirmat afectează prelucrarea efectuată ca persoană subîmputernicită.

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

9. Excepții

9.1.1 [All] Privacy Lead / PIMS Manager TREBUIE să înregistreze orice excepție de la această politică în REG12 înainte de implementare sau în termen de 24 de ore după o acțiune de urgență atunci când aprobarea prealabilă nu a fost posibilă.

9.1.2 [Conditional] Top Management TREBUIE să aprobe orice excepție care afectează în mod semnificativ termenul de notificare a încălcării, termenul de raportare în sectorul financiar, comunicarea publică, angajamentul față de client, păstrarea dovezilor sau riscul pentru persoanele vizate înainte de închiderea incidentului, cu păstrarea dovezilor aprobării în REG10 și REG12.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor TREBUIE să documenteze consilierea pentru orice notificare întârziată, decizie de a nu notifica, excepție de raportare sau abordare excepțională de comunicare înainte de închiderea incidentului, cu păstrarea consilierii în REG10.

9.1.4 [Both] Vendor / Procurement Owner TREBUIE să înregistreze excepțiile furnizorilor, persoanelor împuternicite, persoanelor subîmputernicite, clienților sau prestatorilor externalizați care afectează răspunsul la incidente în sectorul financiar în REG08 și REG12 în termen de cinci zile lucrătoare după identificarea excepției.

9.1.5 [All] Privacy Lead / PIMS Manager TREBUIE să revizuiască cel puțin lunar excepțiile deschise de la această politică până la închidere, cu păstrarea stării revizuirii în REG12.

10. Aplicare

10.1.1 [All] Process Owner / Business Owner TREBUIE să escaladeze neîndeplinirea obligației de a raporta un incident PII suspectat din sectorul financiar, de a păstra dovezi, de a urma acțiunile atribuite sau de a coopera la evaluarea încălcării către Privacy Lead / PIMS Manager în termen de două zile lucrătoare după descoperire, cu păstrarea dovezilor în REG12.

10.1.2 [Both] Incident Response Coordinator TREBUIE să escaladeze raportarea întârziată, clasificarea omisă, dovezile lipsă, escaladarea omisă sau acțiunea de conținere restantă către Privacy Lead / PIMS Manager în termen de o zi lucrătoare după identificarea problemei, cu păstrarea dovezilor în REG10 și REG12.

10.1.3 [Both] Privacy Lead / PIMS Manager TREBUIE să înregistreze o neconformitate REG12 atunci când o încălcare a acestei politici afectează primirea raportării incidentului, triajul, conținerea, notificarea, raportarea, integritatea dovezilor, comunicarea sau acțiunea corectivă.

10.1.4 [Both] Vendor / Procurement Owner TREBUIE să inițieze remedierea de către furnizor, persoana împuternicită, persoana subîmputernicită sau prestatorul externalizat prin REG08 și REG12 în termen de cinci zile lucrătoare atunci când un terț nu respectă obligațiile convenite privind incidentele, încălcările, dovezile sau raportarea.

10.1.5 [Conditional] Top Management TREBUIE să revizuiască neconformitățile PII15-FS semnificative sau recurente la următoarea revizuire de management programată, cu păstrarea deciziilor și a acțiunilor necesare în REG12.

10.1.6 [All] Privacy Lead / PIMS Manager TREBUIE să declanșeze instruire de remediere în REG11 în termen de 30 de zile calendaristice atunci când o neconformitate a politicii implică conștientizarea rolului, raportare întârziată, eșec de escaladare, eșec de gestionare a dovezilor sau eșec de comunicare.

11. Revizuire și întreținere

11.1.1 [Conditional] Privacy Lead / PIMS Manager TREBUIE să revizuiască această politică cel puțin anual și să înregistreze rezultatul revizuirii, modificările necesare și starea aprobării în REG12.

11.1.2 [Conditional] Incident Response Coordinator TREBUIE să declanșeze o revizuire post-incident a acestei politici în termen de 30 de zile calendaristice după închiderea oricărui incident PII cu impact ridicat în sectorul financiar, a oricărei încălcări PII confirmate, a oricărui incident major din sectorul financiar sau a oricărei amenințări cibernetice semnificative, cu păstrarea dovezilor revizuirii în REG10 și REG12.

11.1.3 [Conditional] Privacy Lead / PIMS Manager TREBUIE să revizuiască această politică în termen de 30 de zile calendaristice după ce ia cunoștință de o modificare semnificativă a cerințelor legale, sectoriale, ale clienților, contractuale, ale persoanelor împuternicite, ale persoanelor subîmputernicite, ale modelului de raportare, ale termenului de raportare sau legate de transferuri privind raportarea incidentelor, cu păstrarea dovezilor revizuirii în REG01, REG08, REG09 și REG12.

11.1.4 [Both] Internal Audit / Compliance Reviewer TREBUIE să revizuiască implementarea acestei politici cel puțin anual prin programul de audit intern PIMS, cu păstrarea constatărilor de audit și a acțiunilor corective în REG12.

11.1.5 [Conditional] Top Management TREBUIE să revizuiască tendințele incidentelor, încălcările semnificative, performanța raportării, acțiunile corective restante și eficacitatea politicii în cadrul revizuirii de management programate, cu păstrarea rezultatelor în REG12.

11.1.6 [Conditional] Privacy Lead / PIMS Manager TREBUIE să revizuiască relația de înlocuire dintre PII15-FS și PII15 cel puțin anual și după orice modificare a delimitării domeniului PIMS, pentru a verifica faptul că ambele politici nu sunt implementate pentru același domeniu de aplicare din sectorul financiar, cu păstrarea dovezilor revizuirii în REG03 și REG12.

12. Politici conexe

12.1 Această 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 PII04 - Politica privind nota de informare privind confidențialitatea și transparența

12.1.5 PII06 - Politica de gestionare a drepturilor persoanelor vizate

12.1.6 PII07 - Politica privind evaluarea riscurilor privind confidențialitatea și DPIA

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

12.1.8 PII10 - Politica de păstrare, ștergere și eliminare a PII

12.1.9 PII12 - Politica de management al confidențialității pentru persoanele împuternicite, persoanele subîmputernicite și terți

12.1.10 PII13 - Politica privind transferurile internaționale de PII

12.1.11 PII14 - Politica de securitate și control al accesului pentru PII

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

12.1.13 PII17 - Politica PIMS privind informațiile documentate și gestionarea dovezilor

12.1.14 PII18 - Politica PIMS privind monitorizarea, auditul și îmbunătățirea

12.1.15 PII23 - Politica privind persoana împuternicită PII în cloud, atunci când obligațiile persoanei împuternicite din cloud pentru sectorul financiar sunt incluse în domeniul de aplicare

12.2 PII15 - Politica de gestionare a incidentelor și încălcărilor privind PII este politica de bază privind incidentele și încălcările. PII15-FS este o variantă de înlocuire pentru sectorul financiar a PII15. PII15 și PII15-FS nu trebuie implementate simultan pentru același domeniu de aplicare PIMS, aceeași unitate de business, același produs, mediu de client, serviciu reglementat sau perimetru al dovezilor.

13. Standarde și cadre de referință

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.8; 4.5.1; 4.5.4; 4.5.5; 5.2.2; 7.1.1; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.1.3; 4.2.3; 4.3.1; 4.3.4; 4.3.5; 4.7.3; 6.1.4; 7.1.4].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.7.1; 4.7.2; 4.7.6; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 9.1.1; 10.1.1; 11.1.4; 11.1.5].

13.4 ISO/IEC 27701:2025 - Annex A.3.11. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 5.1.1; 6.1.1; 7.1.2; 7.1.6; 7.1.7].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.6.1; 4.6.2].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 4.5.7; 9.1.2; 11.1.3].

13.7 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.6. Addressed by clauses [4.2.6; 4.2.7; 4.3.6; 4.4.4; 4.4.5; 4.4.10; 4.5.6; 5.7.1; 7.1.3; 8.1.5; 10.1.4].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.5.1; 4.7.2; 5.2.1; 6.1.1; 8.1.2; 11.1.6].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.6; 4.5.1].

13.10 GDPR - Article 28. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3; 10.1.4].

13.11 GDPR - Article 32. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.2; 4.7.3; 7.1.4].

13.12 GDPR - Article 33. Addressed by clauses [4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.5.4; 8.1.2].

13.13 GDPR - Article 34. Addressed by clauses [4.4.3; 4.5.4].

13.14 GDPR - Article 39. Addressed by clauses [4.2.4; 4.4.3; 5.3.1; 6.1.4; 9.1.3].

13.15 DORA Regulation (EU) 2022/2554 - Article 17. Addressed by clauses [4.1.3; 4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.3; 4.3.4; 4.3.6; 4.4.7; 4.5.1; 4.7.1; 5.4.1; 6.1.2; 7.1.7].

13.16 DORA Regulation (EU) 2022/2554 - Article 18. Addressed by clauses [4.2.1; 4.2.2; 4.6.1; 4.6.2; 4.6.3; 8.1.3].

13.17 DORA Regulation (EU) 2022/2554 - Article 19. Addressed by clauses [4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.5; 8.1.3].

13.18 DORA Regulation (EU) 2022/2554 - Article 20. Addressed by clauses [4.4.8; 4.5.5; 6.1.4; 7.1.2; 8.1.3; 11.1.3].

13.19 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.4.7; 4.4.8; 4.5.5; 6.1.4; 8.1.3; 11.1.3].

13.20 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.4.3; 4.5.1; 4.5.3; 4.7.2; 5.2.1; 8.1.2].

13.21 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.7.1].

13.22 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.4; 4.3.6; 4.5.2; 4.7.1; 4.7.2; 7.1.7; 10.1.2].

13.23 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.4; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1.7].

13.24 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.4; 4.1.6; 4.7.1; 4.7.5; 7.1.6; 7.1.7; 10.1.6].

13.25 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.1; 4.7.1].

13.26 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3].