					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: PII15					Titlul documentului: **Politica de gestionare a incidentelor și încălcărilor privind 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 7.4; Clause 7.5	Both	Supporting	Comunicări PIMS și dovezi documentate privind încălcările
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 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 sprijin pentru obligațiile clientului
GDPR	Article 5(2); Article 24	Controller	Supporting	Responsabilitate și răspunderea operatorului
GDPR	Article 26	Joint Controller	Supporting	Coordonarea responsabilității

				operatorilor asociați privind încălcările
GDPR	Article 28	Both	Supporting	Asistența persoanei împuternicite și obligațiile contractuale ale acesteia
GDPR	Article 32	Both	Supporting	Securitatea prelucrării și capacitatea de detectare a încălcărilor
GDPR	Article 33	Both	Primary	Notificarea încălcărilor securității datelor cu caracter personal și documentarea încălcărilor
GDPR	Article 34	Controller	Primary	Comunicarea încălcărilor securității datelor cu caracter personal către persoanele vizate afectate
GDPR	Article 39	Conditional	Supporting	Consiliere DPO, monitorizare, cooperare și sprijin ca punct de contact
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Principii privind securitatea informațiilor și conformitatea în materie de confidențialitate
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 incidentelor, evaluare, răspuns, lecții învățate și

				colectarea dovezilor
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	Politică, plan, conștientizare, testare și lecții 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 de către persoanele împuternicite din cloud și înregistrările încălcărilor
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Raportarea incidentelor semnificative, acolo unde se aplică
DORA Regulation (EU) 2022/2554	Article 17; Article 18; Article 19	Conditional	Supporting	Gestionarea, clasificarea și raportarea incidentelor ICT, acolo unde se aplică

1. Domeniu de aplicare

1.1 Această politică definește cerințele pentru identificarea, raportarea, triajul, evaluarea, conținerea, notificarea, documentarea, închiderea și îmbunătățirea pe baza incidentelor PII și a încălcărilor privind PII în domeniul de aplicare al PIMS.

1.2 Această politică se aplică:

1.2.1 organizației care acționează în calitate de operator PII;

1.2.2 organizației care acționează în calitate de operator asociat, atunci când este necesară coordonarea responsabilității privind încălcările;

1.2.3 organizației care acționează în calitate de persoană împuternicită pentru PII;

1.2.4 organizației care acționează în calitate de persoană subîmputernicită;

1.2.5 sistemelor, aplicațiilor, serviciilor, proceselor, furnizorilor, persoanelor împuternicite, persoanelor subîmputernicite și terților care prelucrează, stochează, transmit, susțin, accesează sau afectează în alt mod PII în domeniul de aplicare al PIMS.

1.3 Această politică utilizează REG10 - Registrul incidentelor și încălcărilor privind PII ca obiect principal de dovezi pentru gestionarea incidentelor și încălcărilor privind PII.

1.4 Această politică utilizează obiecte de dovezi suport după cum urmează:

1.4.1 REG01 pentru domeniul de aplicare al PIMS, părțile interesate aplicabile, precum și contextul legal, contractual, sectorial și de raportare către clienți.

1.4.2 REG02 pentru activitățile de prelucrare afectate, categoriile de PII, categoriile de persoane vizate, scopuri și sisteme.

1.4.3 REG03 pentru Declarație de aplicabilitate și actualizările privind aplicabilitatea controalelor.

1.4.4 REG04 pentru legătura cu riscul privind confidențialitatea, DPIA și riscul rezidual.

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

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

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

1.4.8 REG12 pentru dovezi privind auditul, neconformitatea, acțiunea corectivă și îmbunătățirea.

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

1.5.1 PII03 guvernează inventarul prelucrărilor și înregistrările privind temeiurile juridice.

1.5.2 PII04 guvernează controalele privind notele de informare privind confidențialitatea și transparența în afara comunicărilor specifice încălcărilor.

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

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

1.5.5 PII08 guvernează controalele de protecție a datelor încă din faza de proiectare și în mod implicit.

1.5.6 PII10 guvernează controalele de retenție, ștergere și eliminare.

1.5.7 PII12 guvernează controalele privind relațiile de confidențialitate cu persoanele împuternicite, persoanele subîmputernicite, furnizorii și terții.

1.5.8 PII13 guvernează mecanismele de transfer internațional al PII și înregistrările privind riscurile de transfer.

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

1.5.10 PII16 guvernează instruirea, conștientizarea și competența în materie de confidențialitate.

1.5.11 PII17 guvernează informațiile documentate și gestionarea dovezilor.

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

1.6 În sensul prezentei politici:

1.6.1 „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.

1.6.2 „Încălcare privind PII" înseamnă un incident PII confirmat care implică distrugerea, pierderea, modificarea, divulgarea, accesarea, indisponibilitatea sau compromiterea neautorizată, ilegală, accidentală sau neintenționată a PII.

1.6.3 „Evaluarea încălcării" înseamnă evaluarea documentată a faptului dacă un incident PII este o încălcare privind PII, ce PII și ce persoane vizate sunt afectate, ce riscuri pot apărea, ce notificări sau comunicări sunt necesare și ce acțiuni de remediere sunt necesare.

1.6.4 „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 a fost sau este posibil să fi fost compromis.

1.6.5 „Incident PII cu impact ridicat" înseamnă un incident PII care implică prelucrări cu risc ridicat, categorii speciale sau PII foarte sensibile, PII la scară largă, persoane vulnerabile, clienți reglementați, impact în mai multe jurisdicții, impact material asupra clienților, compromiterea accesului privilegiat, expunere publică, ransomware, indisponibilitatea serviciului sau impact operațional ori reputațional semnificativ.

1.6.6 „Modificare materială a incidentului" înseamnă informații noi sau modificate care afectează domeniul incidentului, severitatea, categoriile de PII, impactul asupra persoanelor vizate, 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 de a asigura că incidentele și încălcările privind PII sunt gestionate consecvent, prompt, legal, sigur și cu dovezi pregătite pentru audit.

2.2 Această politică susține responsabilitatea prin impunerea înregistrării incidentelor și încălcărilor privind PII în REG10 și a legării acestora de înregistrările de prelucrare afectate, riscurile privind confidențialitatea, relațiile cu persoanele împuternicite și subîmputernicite, înregistrările de transfer, acțiunile corective și înregistrările de instruire, atunci când sunt declanșate.

2.3 Această politică asigură că obligațiile operatorului, operatorului asociat, persoanei împuternicite și persoanei subîmputernicite sunt gestionate prin reguli distincte de aplicabilitate, menținând totodată un model integrat de dovezi pentru incidente și încălcări.

3. Obiective

3.1 Obiectivele acestei politici sunt:

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

3.1.2 să asigure trierea și clasificarea incidentelor PII prin criterii consecvente;

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

3.1.4 să asigure documentarea deciziilor privind notificarea de către operator și comunicarea către persoanele vizate;

3.1.5 să asigure efectuarea notificărilor privind încălcările de către persoanele împuternicite și persoanele subîmputernicite către clienți sau părți din amonte fără întârzieri nejustificate și în conformitate cu acordurile aplicabile;

3.1.6 să asigure păstrarea și protejarea dovezilor pe durata gestionării incidentului;

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

3.1.8 să asigure evaluarea declanșatorilor de raportare reglementară, contractuală, către clienți și sectorială, acolo unde se aplică;

3.1.9 să asigure că lecțiile învățate din incidente conduc la acțiune corectivă și îmbunătățire continuă;

3.1.10 să asigure disponibilitatea înregistrărilor privind incidentele și încălcările pentru audit, revizuirea de management, asigurarea solicitată de clienți și revizuirea reglementară, acolo unde se aplică.

4. Declarații de politică

4.1 Pregătirea pentru incidente și preluarea raportărilor

4.1.1 [Both] Privacy Lead / PIMS Manager TREBUIE să mențină criteriile de gestionare a incidentelor și încălcărilor privind PII în REG10 cel puțin anual și după orice modificare semnificativă a domeniului de aplicare al PIMS, a contextului legal, a obligațiilor contractuale sau a prelucrărilor cu risc ridicat.

4.1.2 [All] Incident Response Coordinator TREBUIE să înregistreze fiecare incident PII suspectat 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 sau de raportare către client.

4.1.3 [Both] System Owner / Application Owner TREBUIE să păstreze jurnalele de sistem relevante, alertele, înregistrările de acces, dovezile de configurare și dovezile de recuperare legate de REG10 atunci când un incident suspectat afectează un sistem sau o aplicație care prelucrează PII.

4.1.4 [Both] Information Security Lead TREBUIE să finalizeze triajul tehnic inițial al oricărui eveniment de securitate care implică PII în termen de 24 de ore de la detectare și să înregistreze severitatea inițială, activele afectate și stadiul conținerii în REG10.

4.2 Clasificare și evaluarea încălcării

4.2.1 [Both] Incident Response Coordinator TREBUIE să clasifice fiecare înregistrare REG10 ca eveniment care nu implică PII, incident PII suspectat, incident PII confirmat sau încălcare privind PII confirmată în termen de 24 de ore de la preluare ori să actualizeze înregistrarea REG10 cu motivul pentru care clasificarea rămâne în așteptare.

4.2.2 [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.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor TREBUIE să evalueze riscul pentru persoanele vizate afectate pentru fiecare încălcare privind 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.

4.2.4 [Processor] Privacy Lead / PIMS Manager TREBUIE să identifice operatorul sau clientul afectat și cerințele contractuale de notificare aplicabile de îndată ce organizația ia cunoștință de o încălcare privind PII care afectează PII ale clientului și TREBUIE să înregistreze rezultatul în REG08 și REG10.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager TREBUIE să verifice responsabilitatea agreată privind încălcarea, responsabilitatea principală pentru comunicare și aranjamentul de coordonare înaintea oricărei notificări sau comunicări externe de către un operator asociat și TREBUIE să înregistreze decizia în REG08 și REG10.

4.2.6 [Conditional] Privacy Lead / PIMS Manager TREBUIE să evalueze declanșatorii aplicabili de raportare legală, sectorială, din sectorul financiar, de securitate cibernetică, contractuală, către clienți și către beneficiarii serviciilor pentru fiecare incident PII cu impact ridicat și să înregistreze rezultatul privind aplicabilitatea în REG01, REG08 și REG10.

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

9. Excepții

9.1.1 [Both] 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 fezabilă.

9.1.2 [Both] Top Management TREBUIE să aprobe orice excepție care afectează material calendarul notificării încălcării, comunicarea publică, angajamentul față de client, păstrarea dovezilor sau riscul pentru persoanele vizate înainte de închiderea incidentului, cu păstrarea dovezilor de aprobare în REG10 și REG12.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor TREBUIE să documenteze consilierea pentru orice notificare întârziată, decizie de ne-notificare 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 determinate de furnizori, persoane împuternicite, persoane subîmputernicite sau clienți care afectează răspunsul la incidente în REG08 și REG12 în termen de cinci zile lucrătoare de la identificarea excepției.

10. Respectarea politicii

10.1.1 [All] Process Owner / Business Owner TREBUIE să escaladeze neîndeplinirea obligației de a raporta un incident PII suspectat, 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 de la descoperire, cu păstrarea dovezilor în REG12.

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

10.1.3 [Both] Vendor / Procurement Owner TREBUIE să inițieze remedierea furnizorului sau a persoanei împuternicite prin REG08 și REG12 în termen de cinci zile lucrătoare atunci când o persoană împuternicită, persoană subîmputernicită, furnizor sau alt terț nu își îndeplinește obligațiile agreate privind incidentele sau încălcările.

10.1.4 [Both] Top Management TREBUIE să revizuiască neconformitățile materiale sau recurente privind gestionarea incidentelor la următoarea revizuire de management programată, cu păstrarea deciziilor și acțiunilor necesare în REG12.

11. Revizuire și mentenanță

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

11.1.2 [Both] 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 sau a oricărei încălcări privind PII confirmate, cu păstrarea dovezilor de revizuire în REG10 și REG12.

11.1.3 [Conditional] Privacy Lead / PIMS Manager TREBUIE să revizuiască această politică în termen de 30 de zile calendaristice de la luarea la cunoștință a unei modificări materiale a cerințelor aplicabile de raportare a incidentelor legale, sectoriale, către clienți, contractuale, privind persoanele împuternicite, persoanele subîmputernicite sau legate de transfer, cu păstrarea dovezilor de revizuire 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 [Both] Top Management TREBUIE să revizuiască tendințele incidentelor, încălcările semnificative, performanța notificării, acțiunile corective restante și eficacitatea politicii în timpul revizuirii de management programate, cu păstrarea rezultatelor în REG12.

12. Politici conexe

12.1 Această politică trebuie citită împreună cu:

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

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

12.4 PII03 - Politica privind inventarul prelucrărilor PII și temeiul juridic

12.5 PII04 - Politica privind notele de informare privind confidențialitatea și transparența

12.6 PII06 - Politica de gestionare a drepturilor persoanelor vizate

12.7 PII07 - Politica privind evaluarea riscurilor privind confidențialitatea și DPIA

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

12.9 PII10 - Politica privind retenția, ștergerea și eliminarea PII

12.10 PII12 - Politica de gestionare a confidențialității pentru persoane împuternicite, persoane subîmputernicite și terți

12.11 PII13 - Politica privind transferurile internaționale de PII

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

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

12.14 PII17 - Politica PIMS privind informațiile documentate și gestionarea dovezilor

12.15 PII18 - Politica PIMS privind monitorizarea, auditul și îmbunătățirea

13. Standarde și cadre de referință

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.7; 4.5.1; 4.5.3; 4.5.4; 5.2.2; 6.2.2; 7.1.1; 7.1.7; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.2.2; 4.3.4; 4.6.3; 6.3.1; 7.1.4; 11.1.2].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 6.4.1; 6.5.1; 8.1.1; 8.1.4; 10.1.2; 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; 4.2.6; 4.4.1; 5.1.1; 5.4.1; 7.1.1; 7.1.2; 7.1.6].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.4; 4.2.1; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.3; 4.4.4; 4.5.1; 4.5.4; 6.3.1].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.2.6; 4.4.6; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.4; 6.2.2; 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 [4.2.4; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.2; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 4.6.2; 5.2.1; 6.3.1; 8.1.3; 11.1.5].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.1; 4.4.3; 5.3.1; 6.2.2; 11.1.3].

13.10 GDPR - Article 28. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.11 GDPR - Article 32. Addressed by clauses [4.1.3; 4.1.4; 4.3.2; 4.3.3; 4.5.2; 4.6.3; 5.5.1; 7.1.4; 8.1.2; 11.1.2].

13.12 GDPR - Article 33. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.1; 4.5.4; 8.1.3; 9.1.3].

13.13 GDPR - Article 34. Addressed by clauses [4.2.3; 4.2.5; 4.4.2; 4.4.3; 4.4.7; 4.5.4; 8.1.3; 9.1.3].

13.14 GDPR - Article 39. Addressed by clauses [4.2.3; 4.4.2; 5.3.1; 6.2.2; 9.1.3; 11.1.3].

13.15 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.2.2; 4.3.2; 4.3.3; 4.5.3; 4.6.2; 4.6.3; 5.2.2; 6.4.1; 8.1.4; 11.1.4].

13.16 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.3; 4.6.5; 7.1.3; 7.1.6].

13.17 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.5.1; 4.5.2; 4.6.1; 4.6.2; 7.1.2; 7.1.6].

13.18 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.2; 4.6.1; 5.4.1; 7.1.6; 11.1.2].

13.19 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.1; 4.6.1; 4.6.5; 5.1.1; 7.1.1; 7.1.3; 7.1.6; 8.1.6; 11.1.1; 11.1.2].

13.20 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.1; 4.4.4; 4.5.1; 5.4.2; 6.1.2; 8.1.2].

13.21 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5].

13.22 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.2.6; 4.4.6; 4.4.7; 5.3.1; 6.2.2; 8.1.3; 11.1.3].

13.23 DORA Regulation (EU) 2022/2554 - Article 17; Article 18; Article 19. Addressed by clauses [4.2.1; 4.2.6; 4.4.6; 4.4.7; 5.1.2; 6.2.1; 8.1.3; 11.1.3; 11.1.5].