					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: PII23					Titlul documentului: **Politica privind persoana împuternicită pentru PII în cloud**							
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 / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 4.1; Clause 6.1.3	Processor	Supporting	Rolul PIMS și aplicabilitatea controalelor
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Processor	Primary	Dovezi documentate privind persoana împuternicită în cloud și control operațional
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Processor	Supporting	Monitorizare, neconformitate și acțiune corectivă
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.5; Annex A.2.2.6; Annex A.2.2.7	Processor	Primary	Acorduri cu clienții, instrucțiuni, asistență și înregistrări
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Asistență acordată clienților pentru obligațiile privind persoanele vizate
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Primary	Fișiere temporare, returnare, transfer, eliminare și controale privind transmiterea
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Supporting	Temeiul transferului și locațiile
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Evidențe ale divulgărilor și gestionarea solicitărilor de divulgare
ISO/IEC 27701:2025	Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9	Processor	Primary	Divulgarea persoanelor subîmputernicite, contractarea și notificarea modificărilor
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9; Annex A.3.14; Annex A.3.24; Annex A.3.25	Processor	Supporting	Dovezi privind accesul, înregistrările, backup-ul și jurnalizarea

GDPR	Article 28	Processor	Primary	Persoană împuternicită, persoană subîmputernicită, asistență, audit, ștergere și returnare
GDPR	Article 30	Processor	Supporting	Evidențe ale persoanei împuternicite
GDPR	Article 32; Article 33	Processor	Supporting	Securitate și notificarea încălcării către operator
GDPR	Article 44	Conditional	Referenced	Rutarea transferurilor internaționale
ISO/IEC 29100:2020	Clause 5.3; Clause 5.5; Clause 5.6	Processor	Supporting	Scop, minimizare, utilizare, retenție și limitarea divulgării
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Processor	Supporting	Responsabilitate, securitatea informațiilor și conformitate
ISO/IEC 29151:2022	Clause 15.1.2; Clause 15.2.2; Clause 15.2.3; Annex A.7; Annex A.7.2	Processor	Supporting	Evaluarea persoanei împuternicite, monitorizare, schimbare și controale de retenție
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 5.19; 5.20; 5.21; 5.22; 5.23	Processor	Supporting	Aplicabilitatea controalelor, control operațional și controale privind furnizorii/cloud
ISO/IEC 27002:2022	Control 5.19; Control 5.20; Control 5.21; Control 5.22; Control 5.23; Control 8.10; Control 8.15; Control 8.16	Processor	Supporting	Controale privind furnizorii, cloud-ul, ștergerea, jurnalizarea și monitorizarea
ISO/IEC 27018:2020	Annex A.2.1; Annex A.3.1	Processor	Primary	Asistență pentru clienți din partea persoanei împuternicite în

				cloud și limitarea scopului
ISO/IEC 27018:2020	Annex A.6.1; Annex A.6.2; Annex A.8.1	Processor	Primary	Notificarea divulgării în cloud, evidențe ale divulgărilor și transparența persoanelor subîmputernicite
ISO/IEC 27018:2020	Annex A.10.1; Annex A.10.3; Annex A.11.11; Annex A.11.12; Annex A.12.1	Processor	Primary	Interfața pentru încălcări în cloud, ieșire, măsuri contractuale, subcontracte și evidențe ale locațiilor
ISO/IEC 27036-2:2022	Clause 6.1.1; Clause 6.1.2	Processor	Supporting	Strategia și guvernanța relațiilor de aprovizionare
ISO/IEC 27036-2:2022	Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5	Processor	Supporting	Planificarea, acordul, managementul, monitorizarea și încetarea relației cu furnizorul
ISO/IEC 27555:2025	Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8	Processor	Supporting	Cadrul de ștergere și documentarea
ISO/IEC 27555:2025	Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7	Processor	Supporting	Implementarea ștergerii și excepții

1. Domeniu de aplicare

1.1 Prezenta politică definește cerințele obligatorii de confidențialitate pentru serviciile cloud în cadrul cărora organizația acționează ca persoană împuternicită sau persoană subîmputernicită pentru PII, inclusiv servicii SaaS, PaaS, IaaS, aplicații găzduite, cloud administrat, suport cloud, stocare cloud, analiză cloud și servicii de infrastructură cloud care prelucrează PII în numele clienților.

1.2 Prezenta politică se aplică prelucrării în cloud efectuate în baza acordurilor cu clienții, a instrucțiunilor documentate ale clienților, a instrucțiunilor persoanelor împuternicite din amonte, a relațiilor cu persoanele subîmputernicite, a configurării regiunilor cloud, a accesului pentru suport cloud, a administrării serviciilor, backup-ului, replicării, jurnalizării, monitorizării, ștergerii, returnării, suportului pentru încălcări, suportului pentru audit și obligațiilor de asistență pentru clienți.

1.3 Prezenta politică acoperă:

1.3.1 domeniul de aplicare al prelucrării PII în cloud și înregistrările instrucțiunilor;

1.3.2 acordurile cu clienții și dovezile privind responsabilitatea partajată;

1.3.3 izolarea tenanturilor, accesul cloud, accesul administrativ și dovezile de jurnalizare;

1.3.4 guvernanța persoanelor subîmputernicite și a lanțului de aprovizionare cloud;

1.3.5 locația, accesul la distanță și rutarea transferurilor internaționale;

1.3.6 dovezile privind returnarea, transferul, ștergerea, eliminarea și ieșirea;

1.3.7 asistența pentru clienți privind drepturile persoanelor vizate, DPIA, auditurile și răspunsul la încălcări;

1.3.8 dovezile privind monitorizarea, excepțiile, aplicarea și îmbunătățirea.

1.4 Prezenta politică nu creează un registru separat al contractelor cu clienții, un registru al serviciilor cloud, un registru al izolării tenanturilor, un registru de acces, un registru de jurnale, un registru de ștergere, un registru al solicitărilor de suport, un registru al dovezilor de audit, un registru al încălcărilor, un registru al persoanelor subîmputernicite sau un comitet de guvernanță cloud.

1.5 Prezenta politică nu înlocuiește:

1.5.1 PII03 pentru inventarul prelucrării și deținerea temeiului juridic;

1.5.2 PII06 pentru fluxul complet de lucru privind drepturile persoanelor vizate;

1.5.3 PII07 pentru metodologia privind riscurile de confidențialitate și DPIA;

1.5.4 PII08 pentru punctele de control privind protecția datelor încă din faza de proiectare și protecția datelor în mod implicit;

1.5.5 PII09 pentru controalele generale privind colectarea, utilizarea, divulgarea și partajarea;

1.5.6 PII10 pentru metodologia privind retenția, ștergerea și eliminarea;

1.5.7 PII12 pentru guvernanța generală a ciclului de viață al persoanelor împuternicite, persoanelor subîmputernicite și terților;

1.5.8 PII13 pentru evaluarea mecanismelor de transfer internațional;

1.5.9 PII14 pentru arhitectura completă de securitate și control al accesului pentru PII;

1.5.10 PII15 pentru fluxul de lucru privind gestionarea incidentelor și încălcărilor;

1.5.11 PII17 pentru controlul informațiilor documentate;

1.5.12 PII18 pentru guvernanța monitorizării, auditului și îmbunătățirii PIMS.

2. Scop

2.1 Scopul prezentei politici este de a asigura că serviciile de persoană împuternicită și persoană subîmputernicită pentru PII în cloud sunt operate în baza instrucțiunilor documentate ale clienților, a unui domeniu clar de prelucrare, a unor relații controlate cu persoanele subîmputernicite, a unor responsabilități adecvate de securitate cloud, a locațiilor și rutării transferurilor documentate, a

obligațiilor de asistență pentru clienți, a suportului pentru încălcări, a capabilității de ștergere/returnare și a dovezilor pregătite pentru audit.

2.2 Prezenta politică susține pregătirea pentru certificare ISO/IEC 27701:2025 PIMS pentru persoanele împuternicite în cloud și persoanele subîmputernicite în cloud, rămânând integrată cu setul existent de politici PIMS și cu obiectele canonice de dovezi.

3. Obiective

3.1 Obiectivele prezentei politici sunt:

3.1.1 Să definească domeniul de aplicare al prelucrării PII în cloud înainte de integrarea clientului sau de o modificare semnificativă.

3.1.2 Să asigure că instrucțiunile clienților sunt înregistrate, revizuite și respectate.

3.1.3 Să mențină dovezi privind persoanele împuternicite și persoanele subîmputernicite în cloud în registrele canonice PIMS.

3.1.4 Să definească dovezile privind responsabilitatea partajată, izolarea tenanturilor, accesul, jurnalizarea și locația fără a dubla politica de securitate PII.

3.1.5 Să controleze dovezile privind integrarea, modificarea, obligațiile transmise în lanț și monitorizarea persoanelor subîmputernicite.

3.1.6 Să sprijine clienții în legătură cu drepturile persoanelor vizate, DPIA, solicitările de audit și răspunsul la încălcări.

3.1.7 Să asigure păstrarea dovezilor privind returnarea, ștergerea, transferul și eliminarea la ieșire.

3.1.8 Să monitorizeze controalele persoanei împuternicite în cloud și să impulsioneze acțiunile corective utilizând REG12.

4. Declarații de politică

4.1 Domeniul prelucrării în cloud și instrucțiunile clienților

4.1.1 [Processor] Privacy Lead / PIMS Manager trebuie să înregistreze fiecare serviciu de prelucrare PII în cloud, rolul de prelucrare al clientului, sursa instrucțiunilor clientului, categoriile de PII, categoriile de persoane vizate, scopul serviciului, locația prelucrării, dependența de persoane subîmputernicite, dependența de ștergere și indicatorul de transfer în REG02 și REG08 înainte de integrarea clientului sau de o modificare semnificativă a serviciului.

4.1.2 [Processor] Process Owner / Business Owner trebuie să înregistreze instrucțiunile documentate ale clientului pentru prelucrarea PII în cloud în REG08 înainte de începerea prelucrării.

4.1.3 [Subprocessor] Process Owner / Business Owner trebuie să înregistreze instrucțiunile persoanei împuternicite din amonte sau instrucțiunile aprobate de client în REG08 înainte de a prelucra PII ca persoană subîmputernicită în cloud.

4.1.4 [Processor] Privacy Lead / PIMS Manager trebuie să înregistreze aplicabilitatea controalelor pentru persoana împuternicită în cloud în REG03 înainte ca un nou serviciu de prelucrare PII în cloud să fie lansat sau modificat semnificativ.

4.1.5 [Processor] Data Protection Officer / Privacy Advisor trebuie să revizuiască în REG12 orice instrucțiune a clientului care pare incompatibilă cu obligațiile documentate ale clientului, cerințele PIMS sau domeniul de aplicare aprobat al serviciului, înainte ca organizația să acționeze pe baza instrucțiunii.

4.1.6 [Processor] Process Owner / Business Owner trebuie să înregistreze în REG12 orice prelucrare propusă a PII ale clientului în afara instrucțiunilor documentate ale clientului și să obțină aprobarea Privacy Lead / PIMS Manager înainte ca prelucrarea să aibă loc.

4.2 Configurarea cloud, izolarea tenanturilor, accesul și jurnalizarea

4.2.1 [Processor] Information Security Lead trebuie să înregistreze în REG08 limita responsabilității partajate în cloud pentru accesul la PII, administrare, jurnalizare, backup, criptare, managementul vulnerabilităților și ștergere, înainte de integrarea clientului sau de o modificare semnificativă a serviciului.

4.2.2 [Processor] System Owner / Application Owner trebuie să valideze controalele de izolare a tenanturilor sau de segregare a clienților în REG12 înainte de utilizarea în producție și după o modificare semnificativă a arhitecturii.

4.2.3 [Processor] System Owner / Application Owner trebuie să acorde acces administrativ în cloud la PII ale clienților numai după ce nevoia de afaceri aprobată, domeniul accesului, durata accesului și frecvența revizuirii sunt înregistrate în REG12.

4.2.4 [Processor] Information Security Lead trebuie să revizuiască accesul privilegiat în cloud, accesul de suport, accesul la PII ale clienților și acoperirea jurnalizării în REG12 cel puțin trimestrial.

4.2.5 [Processor] System Owner / Application Owner trebuie să valideze separarea mediilor de producție, staging, testare și suport pentru PII ale clienților în REG12 înainte de lansare și după o modificare semnificativă a mediului.

4.2.6 [Processor] System Owner / Application Owner trebuie să înregistreze locațiile de backup, replicare, stocare a jurnalelor și acces de suport pentru PII ale clienților din cloud în REG02, REG08 sau REG09 înainte de activarea sau modificarea acestor locații.

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

9. Excepții

9.1 [Processor] Process Owner / Business Owner trebuie să solicite o excepție privind persoana împuternicită în cloud în REG12 înainte de integrare, lansare, reînnoire sau utilizare continuă atunci când dovezile necesare privind instrucțiunile clientului, persoana subîmputernicită, locația, accesul, jurnalizarea, ștergerea sau interfața de incident sunt incomplete.

9.2 [Processor] Data Protection Officer / Privacy Advisor trebuie să revizuiască în REG12 solicitările de excepție privind persoana împuternicită în cloud semnificative din perspectiva confidențialității înainte de aprobare, atunci când excepția afectează instrucțiunile clienților, asistența pentru persoanele vizate, transferurile, persoanele subîmputernicite, ștergerea, suportul pentru încălcări sau PII cu impact ridicat.

9.3 [Processor] Top Management trebuie să aprobe excepțiile cu risc ridicat sau semnificative privind persoana împuternicită în cloud în REG12 înainte ca excepția să producă efecte.

9.4 [Processor] Privacy Lead / PIMS Manager trebuie să atribuie în REG12 o dată de expirare, un responsabil de remediere, o dată de revizuire și o notă privind riscul rezidual pentru fiecare excepție aprobată privind persoana împuternicită în cloud înainte de aprobare.

10. Aplicare

10.1 [Processor] Privacy Lead / PIMS Manager trebuie să blocheze integrarea clientului, lansarea serviciului, reînnoirea sau continuarea prelucrării atunci când dovezile necesare REG02, REG03, REG08, REG09, REG10 sau REG12 lipsesc înainte ca prelucrarea să înceapă sau să continue.

10.2 [Processor] System Owner / Application Owner trebuie să dezactiveze accesul cloud neaprobat, utilizarea neaprobată a regiunii, replicarea neaprobată, accesul de suport neaprobat sau fluxul de date neaprobat către persoana subîmputernicită în termen de o zi lucrătoare după o decizie de aplicare și să înregistreze finalizarea în REG08 sau REG12.

10.3 [Processor] Vendor / Procurement Owner trebuie să suspende prelucrarea nouă de PII de către o persoană subîmputernicită în cloud neaprobată sau neconformă până când dovezile privind acțiunea corectivă în REG08 sunt complete.

10.4 [Processor] Incident Response Coordinator trebuie să escaladeze termenele ratate de notificare a incidentelor către clienți în REG10 și REG12 în termen de o zi lucrătoare de la identificare.

10.5 [Processor] Internal Audit / Compliance Reviewer trebuie să verifice eficacitatea acțiunilor corective pentru neconformitățile majore sau repetate privind persoana împuternicită în cloud în REG12 în termen de 60 de zile după închiderea acțiunii corective.

11. Revizuire și întreținere

11.1 [Processor] Privacy Lead / PIMS Manager trebuie să revizuiască prezenta politică în REG12 anual și în termen de 30 de zile după o modificare semnificativă a obligațiilor persoanei împuternicite în cloud, arhitecturii cloud, guvernanței persoanelor subîmputernicite, asistenței pentru clienți, capabilității de ștergere sau cerințelor de certificare.

11.2 [Processor] Vendor / Procurement Owner trebuie să revizuiască înregistrările privind persoanele subîmputernicite în cloud și dependențele de servicii cloud în REG08 cel puțin anual și înainte de reînnoire.

11.3 [Processor] System Owner / Application Owner trebuie să revizuiască dovezile privind izolarea tenanturilor, accesul privilegiat, jurnalizarea, backup-ul, replicarea și ștergerea în REG12 cel puțin anual și după o modificare semnificativă a arhitecturii.

11.4 [Processor] Privacy Lead / PIMS Manager trebuie să revizuiască înregistrările REG09 privind locațiile cloud și rutarea transferurilor cel puțin anual și în termen de 15 zile lucrătoare după o modificare semnificativă a locației, accesului de suport, backup-ului sau persoanei subîmputernicite.

11.5 [Processor] Privacy Lead / PIMS Manager trebuie să actualizeze REG03 în termen de 15 zile lucrătoare după modificările aprobate ale politicii care afectează aplicabilitatea controalelor privind persoana împuternicită în cloud.

11.6 [All] Top Management trebuie să aprobe revizuirile semnificative ale prezentei politici în REG12 înainte de publicare.

12. Politici conexe

12.1 Prezenta politică este susținută de următoarele politici conexe:

12.2 PII01 - Politica sistemului de management al informațiilor privind confidențialitatea

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

12.4 PII03 - Politica privind inventarul prelucrărilor PII și temeiul juridic

12.5 PII06 - Politica de management al drepturilor persoanelor vizate

12.6 PII07 - Politica privind evaluarea riscurilor de confidențialitate și DPIA

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

12.8 PII09 - Politica privind colectarea, utilizarea, divulgarea și partajarea PII

12.9 PII10 - Politica privind retenția, ștergerea și eliminarea PII

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

12.11 PII13 - Politica privind transferul internațional de PII

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

12.13 PII15 - Politica de management al incidentelor și încălcărilor privind PII

12.14 PII17 - Politica de management al informațiilor documentate și dovezilor PIMS

12.15 PII18 - Politica de monitorizare, audit și îmbunătățire PIMS

12.16 PII20 - Politica privind confidențialitatea copiilor

12.17 PII21 - Politica de confidențialitate privind AI și procesul decizional automatizat

12.18 PII22 - Politica de confidențialitate privind marketingul și cookie-urile

12.19 PII24 - Politica de confidențialitate privind CCTV și monitorizarea fizică

13. Standarde și cadre de referință

13.1 Prezenta 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 - Clause 4.1; Clause 6.1.3. Addressed by clauses [4.1.1; 4.1.4; 5.2; 7.1; 11.5].

13.3 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.3.1; 4.4.1; 4.6.1; 4.7.1; 4.8.1; 7.1; 7.2; 7.3].

13.4 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.3.5; 4.6.6; 4.8.1; 4.8.2; 4.8.4; 6.1; 6.2; 8.1; 8.2; 8.3; 8.4; 8.5; 10.5; 11.1].

13.5 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.5; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.2; 4.1.3; 4.1.5; 4.1.6; 4.3.1; 4.7.5; 7.2].

13.6 ISO/IEC 27701:2025 - Annex A.2.3.2. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5].

13.7 ISO/IEC 27701:2025 - Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.8 ISO/IEC 27701:2025 - Annex A.2.5.2; Annex A.2.5.3. Addressed by clauses [4.2.6; 4.4.4; 4.5.1; 4.5.2; 7.5; 11.4].

13.9 ISO/IEC 27701:2025 - Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.5.3; 4.5.4; 4.7.2; 4.7.5].

13.10 ISO/IEC 27701:2025 - Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6].

13.11 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9; Annex A.3.14; Annex A.3.24; Annex A.3.25. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.7.3; 5.4; 5.6; 11.3].

13.12 GDPR - Article 28. Addressed by clauses [4.1.2; 4.1.3; 4.3.1; 4.3.2; 4.3.4; 4.4.2; 4.4.3; 4.4.5; 4.6.1; 4.6.3; 4.6.5; 4.7.2].

13.13 GDPR - Article 30. Addressed by clauses [4.1.1; 4.1.3; 4.4.1; 4.8.1; 7.1].

13.14 GDPR - Article 32; Article 33. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 7.6].

13.15 GDPR - Article 44. Addressed by clauses [4.2.6; 4.4.4; 4.5.1; 4.5.2; 7.5; 11.4].

13.16 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.1.6; 4.2.6; 4.5.1; 4.6.1; 4.6.3].

13.17 ISO/IEC 29100:2020 - Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.4; 4.3.5; 4.8.1; 4.8.4; 6.1; 8.5; 10.5].

13.18 ISO/IEC 29151:2022 - Clause 15.1.2; Clause 15.2.2; Clause 15.2.3; Annex A.7; Annex A.7.2. Addressed by clauses [4.4.1; 4.4.6; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.8.3].

13.19 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 5.19; 5.20; 5.21; 5.22; 5.23. Addressed by clauses [4.1.4; 4.2.1; 4.4.1; 4.4.3; 4.4.6; 4.8.1; 4.8.3; 6.1; 7.1; 11.5].

13.20 ISO/IEC 27002:2022 - Control 5.19; Control 5.20; Control 5.21; Control 5.22; Control 5.23; Control 8.10; Control 8.15; Control 8.16. Addressed by clauses [4.2.1; 4.2.4; 4.4.1; 4.4.3; 4.4.6; 4.6.1; 4.6.3; 4.7.3; 4.8.3; 11.3].

13.21 ISO/IEC 27018:2020 - Annex A.2.1; Annex A.3.1. Addressed by clauses [4.1.2; 4.1.6; 4.3.1; 4.3.2; 4.3.3; 4.3.5].

13.22 ISO/IEC 27018:2020 - Annex A.6.1; Annex A.6.2; Annex A.8.1. Addressed by clauses [4.4.1; 4.4.2; 4.4.5; 4.5.3; 4.5.4].

13.23 ISO/IEC 27018:2020 - Annex A.10.1; Annex A.10.3; Annex A.11.11; Annex A.11.12; Annex A.12.1. Addressed by clauses [4.2.6; 4.4.3; 4.4.4; 4.6.1; 4.6.3; 4.6.5; 4.7.1; 4.7.2; 4.7.5].

13.24 ISO/IEC 27036-2:2022 - Clause 6.1.1; Clause 6.1.2. Addressed by clauses [4.1.1; 4.2.1; 4.4.1; 4.4.6; 6.1; 7.2].

13.25 ISO/IEC 27036-2:2022 - Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.4.6; 4.8.2; 4.8.3; 10.3; 11.2].

13.26 ISO/IEC 27555:2025 - Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.27 ISO/IEC 27555:2025 - Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7. Addressed by clauses [4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6; 9.1; 9.4].