					Sem vložte název registrované právnické osoby							
Číslo dokumentu: PII23					Název dokumentu: **Politika cloudového zpracovatele PII**							
Verze: 1.0		Datum účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Standard		Postup		Formulář		Registr		Jiné	

Historie revizí				
Číslo revize	**Datum revize**	**Změny**	**Přezkoumal**	**Vlastník procesu**

Schválení			
Jméno	**Funkce**	**Datum**	**Podpis**

V souladu s normami a právními předpisy

Norma / právní předpis	Kapitola / opatření / článek	Použitelnost	Typ pokrytí	Komentář
ISO/IEC 27701:2025	Clause 4.1; Clause 6.1.3	Processor	Supporting	Role PIMS a použitelnost opatření
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Processor	Primary	Dokumentované důkazy o cloudovém zpracovateli a operativní řízení
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Processor	Supporting	Monitorování, neshoda a nápravné opatření
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	Smlouvy se zákazníky, pokyny, podpora a záznamy
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Součinnost zákazníkovi při povinnostech vůči subjektům PII
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Primary	Dočasné soubory, vrácení, předání, likvidace a opatření pro přenos
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Supporting	Základ předávání a umístění
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Záznamy o zpřístupnění a vyřizování žádostí o zpřístupnění
ISO/IEC 27701:2025	Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9	Processor	Primary	Zpřístupnění dílčího zpracovatele, zapojení a oznámení změny
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	Přístup, záznamy, zálohování a důkazy o protokolování
GDPR	Article 28	Processor	Primary	Zpracovatel, dílčí zpracovatel, součinnost, audit, výmaz a vrácení

GDPR	Article 30	Processor	Supporting	Záznamy zpracovatele
GDPR	Article 32; Article 33	Processor	Supporting	Zabezpečení a oznámení porušení zabezpečení správci
GDPR	Article 44	Conditional	Referenced	Směrování mezinárodního předávání
ISO/IEC 29100:2020	Clause 5.3; Clause 5.5; Clause 5.6	Processor	Supporting	Účel, minimalizace, použití, uchovávání a omezení zpřístupnění
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Processor	Supporting	Odpovědnost, bezpečnost informací a soulad
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	Hodnocení zpracovatele, monitorování, změna a opatření pro uchovávání
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	Použitelnost opatření, operativní řízení a opatření pro dodavatele/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	Opatření pro dodavatele, cloud, mazání, protokolování a monitorování
ISO/IEC 27018:2020	Annex A.2.1; Annex A.3.1	Processor	Primary	Součinnost cloudového zpracovatele zákazníkovi a omezení účelu
ISO/IEC 27018:2020	Annex A.6.1; Annex A.6.2; Annex A.8.1	Processor	Primary	Cloudové oznamování zpřístupnění, záznamy o zpřístupnění a transparentnost dílčích zpracovatelů

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	Cloudové rozhraní pro porušení zabezpečení, ukončení, smluvní opatření, dílčí smlouvy a záznamy o umístění
ISO/IEC 27036-2:2022	Clause 6.1.1; Clause 6.1.2	Processor	Supporting	Strategie a správa dodavatelského vztahu
ISO/IEC 27036-2:2022	Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5	Processor	Supporting	Plánování, smlouva, řízení, monitorování a ukončení vztahu s dodavatelem
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	Rámec mazání a dokumentace
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	Implementace mazání a výjimky

1. Rozsah

1.1 Tato politika stanoví povinné požadavky na ochranu soukromí pro cloudové služby, u nichž organizace vystupuje jako zpracovatel PII nebo dílčí zpracovatel, včetně služeb SaaS, PaaS, IaaS, hostovaných aplikací, spravovaného cloudu, cloudové podpory, cloudového úložiště, cloudové analytiky a služeb cloudové infrastruktury, které zpracovávají PII jménem zákazníků.

1.2 Tato politika se vztahuje na cloudové zpracování prováděné na základě smluv se zákazníky, dokumentovaných pokynů zákazníků, pokynů předřazeného zpracovatele, ujednání s dílčími zpracovateli, konfigurace cloudových regionů, přístupu cloudové podpory, správy služeb, zálohování, replikace, protokolování, monitorování, mazání, vrácení, podpory při porušení zabezpečení, podpory auditu a povinností součinnosti zákazníkovi.

1.3 Tato politika pokrývá následující oblasti:

1.3.1 rozsah cloudového zpracování PII a záznamy pokynů;

1.3.2 smlouvy se zákazníky a důkazy o sdílené odpovědnosti;

1.3.3 důkazy o izolaci tenantů, cloudovém přístupu, administrátorském přístupu a protokolování;

1.3.4 správu dílčích zpracovatelů a cloudového dodavatelského řetězce;

1.3.5 umístění, vzdálený přístup a směrování mezinárodních předávání;

1.3.6 důkazy o vrácení, předání, výmazu, likvidaci a ukončení;

1.3.7 součinnost zákazníkovi při právech subjektů PII, DPIA, auditech a reakci na porušení zabezpečení;

1.3.8 důkazy o monitorování, výjimkách, prosazování požadavků a zlepšování.

1.4 Tato politika nezavádí samostatný registr zákaznických smluv, registr cloudových služeb, registr izolace tenantů, registr přístupů, registr logů, registr mazání, registr požadavků podpory, registr auditních důkazů, registr porušení zabezpečení, registr dílčích zpracovatelů ani výbor pro správu cloudu.

1.5 Tato politika nenahrazuje následující politiky:

1.5.1 PII03 pro evidenci činností zpracování a vlastnictví právního základu;

1.5.2 PII06 pro úplný pracovní postup práv subjektů PII;

1.5.3 PII07 pro metodiku posouzení rizik pro soukromí a DPIA;

1.5.4 PII08 pro brány ochrany soukromí již od návrhu a ve výchozím nastavení;

1.5.5 PII09 pro obecná opatření pro shromažďování, použití, zpřístupnění a sdílení;

1.5.6 PII10 pro metodiku uchovávání, výmazu a likvidace;

1.5.7 PII12 pro obecnou správu životního cyklu zpracovatelů, dílčích zpracovatelů a třetích stran;

1.5.8 PII13 pro posouzení mechanismu mezinárodního předávání;

1.5.9 PII14 pro úplnou architekturu zabezpečení PII a řízení přístupu;

1.5.10 PII15 pro pracovní postup řízení incidentů a porušení zabezpečení;

1.5.11 PII17 pro řízení dokumentovaných informací;

1.5.12 PII18 pro správu monitorování, auditu a zlepšování PIMS.

2. Účel

2.1 Účelem této politiky je zajistit, aby služby cloudového zpracovatele PII a dílčího zpracovatele byly provozovány na základě dokumentovaných pokynů zákazníka, jasného rozsahu zpracování, řízených ujednání s dílčími zpracovateli, odpovídajících cloudových odpovědností za bezpečnost, dokumentovaného umístění a směrování předávání, povinností součinnosti zákazníkovi, podpory při porušení zabezpečení, schopnosti výmazu/vrácení a důkazů připravených pro audit.

2.2 Tato politika podporuje připravenost na certifikaci PIMS podle ISO/IEC 27701:2025 pro cloudové zpracovatele a cloudové dílčí zpracovatele a současně zůstává integrována se stávajícím souborem politik PIMS a kanonickými důkazními objekty.

3. Cíle

3.1 Cílem této politiky je:

3.1.1 Definovat rozsah cloudového zpracování PII před onboardingem zákazníka nebo významnou změnou.

3.1.2 Zajistit, aby pokyny zákazníka byly zaznamenány, přezkoumány a dodržovány.

3.1.3 Udržovat důkazy o cloudovém zpracovateli a dílčím zpracovateli v kanonických registrech PIMS.

3.1.4 Definovat důkazy o sdílené odpovědnosti, izolaci tenantů, přístupu, protokolování a umístění bez duplicit vůči politice zabezpečení PII.

3.1.5 Řídit důkazy o onboardingu, změně, přenesených povinnostech a monitorování dílčích zpracovatelů.

3.1.6 Poskytovat zákazníkům podporu při právech subjektů PII, DPIA, žádostech o audit a reakci na porušení zabezpečení.

3.1.7 Zajistit, aby při ukončení byly uchovány důkazy o vrácení, výmazu, předání a likvidaci.

3.1.8 Monitorovat opatření cloudového zpracovatele a řídit nápravná opatření pomocí REG12.

4. Prohlášení politiky

4.1 Rozsah cloudového zpracování a pokyny zákazníka

4.1.1 [Processor] Privacy Lead / PIMS Manager musí zaznamenat každou službu cloudového zpracování PII, roli zpracování zákazníka, zdroj pokynu zákazníka, kategorie PII, kategorie subjektů PII, účel služby, místo zpracování, závislost na dílčím zpracovateli, závislost na výmazu a příznak předávání v REG02 a REG08 před onboardingem zákazníka nebo významnou změnou služby.

4.1.2 [Processor] Process Owner / Business Owner musí před zahájením zpracování zaznamenat dokumentované pokyny zákazníka ke cloudovému zpracování PII v REG08.

4.1.3 [Subprocessor] Process Owner / Business Owner musí před zpracováním PII jako cloudový dílčí zpracovatel zaznamenat v REG08 pokyny předřazeného zpracovatele nebo pokyny schválené zákazníkem.

4.1.4 [Processor] Privacy Lead / PIMS Manager musí před vydáním nové služby cloudového zpracování PII nebo její významnou změnou zaznamenat použitelnost opatření cloudového zpracovatele v REG03.

4.1.5 [Processor] Data Protection Officer / Privacy Advisor musí předtím, než organizace podle pokynu postupuje, přezkoumat v REG12 jakýkoli pokyn zákazníka, který se jeví jako neslučitelný s dokumentovanými povinnostmi zákazníka, požadavky PIMS nebo schváleným rozsahem služby.

4.1.6 [Processor] Process Owner / Business Owner musí zaznamenat v REG12 jakékoli navrhované zpracování PII zákazníka mimo dokumentované pokyny zákazníka a získat schválení Privacy Lead / PIMS Manager předtím, než ke zpracování dojde.

4.2 Cloudová konfigurace, izolace tenantů, přístup a protokolování

4.2.1 [Processor] Information Security Lead musí před onboardingem zákazníka nebo významnou změnou služby zaznamenat v REG08 hranici sdílené odpovědnosti v cloudu pro přístup k PII, správu, protokolování, zálohování, šifrování, řízení zranitelností a výmaz.

4.2.2 [Processor] System Owner / Application Owner musí ověřit opatření pro izolaci tenantů nebo oddělení zákazníků v REG12 před produkčním použitím a po významné změně architektury.

4.2.3 [Processor] System Owner / Application Owner smí udělit cloudový administrátorský přístup k PII zákazníka pouze poté, co jsou v REG12 zaznamenány schválená obchodní potřeba, rozsah přístupu, doba trvání přístupu a četnost přezkumu.

4.2.4 [Processor] Information Security Lead musí nejméně čtvrtletně přezkoumat v REG12 privilegovaný cloudový přístup, přístup podpory, přístup k PII zákazníka a pokrytí protokolováním.

4.2.5 [Processor] System Owner / Application Owner musí ověřit oddělení produkčních, staging, testovacích a podpůrných prostředí pro PII zákazníka v REG12 před vydáním a po významné změně prostředí.

4.2.6 [Processor] System Owner / Application Owner musí před povolením nebo změnou těchto umístění zaznamenat umístění záloh, replikací, úložišť logů a přístupu podpory pro cloudové PII zákazníka v REG02, REG08 nebo REG09.

[... Oddíly 4.3–8 nejsou součástí tohoto náhledu. Pro přístup k úplnému obsahu zakupte celý dokument. ...]

9. Výjimky

9.1 [Processor] Process Owner / Business Owner musí před onboardingem, vydáním, obnovením nebo pokračujícím použitím požádat v REG12 o výjimku cloudového zpracovatele, pokud jsou neúplné požadované důkazy o pokynu zákazníka, dílčím zpracovateli, umístění, přístupu, protokolování, výmazu nebo rozhraní incidentů.

9.2 [Processor] Data Protection Officer / Privacy Advisor musí před schválením přezkoumat v REG12 žádosti o výjimku cloudového zpracovatele významné z hlediska ochrany osobních údajů, pokud výjimka ovlivňuje pokyny zákazníka, součinnost při právech subjektů PII, předávání, dílčí zpracovatele, výmaz, podporu při porušení zabezpečení nebo PII s vysokým dopadem.

9.3 [Processor] Top Management musí před nabytím účinnosti výjimky schválit v REG12 vysoce rizikové nebo významné výjimky cloudového zpracovatele.

9.4 [Processor] Privacy Lead / PIMS Manager musí před schválením přiřadit v REG12 ke každé schválené výjimce cloudového zpracovatele datum konce platnosti, vlastníka nápravy, datum přezkumu a poznámku ke zbytkovému riziku.

10. Prosazování požadavků

10.1 [Processor] Privacy Lead / PIMS Manager musí zablokovat onboarding zákazníka, vydání služby, obnovení nebo pokračující zpracování, pokud před zahájením nebo pokračováním zpracování chybí požadované důkazy REG02, REG03, REG08, REG09, REG10 nebo REG12.

10.2 [Processor] System Owner / Application Owner musí do jednoho pracovního dne po rozhodnutí o prosazení požadavků deaktivovat neschválený cloudový přístup, neschválené použití regionu, neschválenou replikaci, neschválený přístup podpory nebo neschválený datový tok k dílčímu zpracovateli a zaznamenat dokončení v REG08 nebo REG12.

10.3 [Processor] Vendor / Procurement Owner musí pozastavit nové zpracování PII neschváleným nebo nevyhovujícím cloudovým dílčím zpracovatelem, dokud nejsou úplné důkazy o nápravném opatření v REG08.

10.4 [Processor] Incident Response Coordinator musí do jednoho pracovního dne po identifikaci eskalovat zmeškané lhůty pro oznámení incidentu zákazníkovi v REG10 a REG12.

10.5 [Processor] Internal Audit / Compliance Reviewer musí do 60 dnů po uzavření nápravného opatření ověřit účinnost nápravného opatření u závažných nebo opakovaných neshod cloudového zpracovatele v REG12.

11. Přezkum a údržba

11.1 [Processor] Privacy Lead / PIMS Manager musí každoročně a do 30 dnů po významné změně povinností cloudového zpracovatele, cloudové architektury, správy dílčích zpracovatelů, součinnosti zákazníkovi, schopnosti výmazu nebo certifikačních požadavků přezkoumat tuto politiku v REG12.

11.2 [Processor] Vendor / Procurement Owner musí nejméně jednou ročně a před obnovením přezkoumat záznamy cloudových dílčích zpracovatelů a závislostí na cloudových službách v REG08.

11.3 [Processor] System Owner / Application Owner musí nejméně jednou ročně a po významné změně architektury přezkoumat v REG12 důkazy o izolaci tenantů, privilegovaném přístupu, protokolování, zálohování, replikaci a výmazu.

11.4 [Processor] Privacy Lead / PIMS Manager musí nejméně jednou ročně a do 15 pracovních dnů po významné změně umístění, přístupu podpory, zálohování nebo dílčího zpracovatele přezkoumat záznamy cloudových umístění a směrování předávání v REG09.

11.5 [Processor] Privacy Lead / PIMS Manager musí do 15 pracovních dnů po schválených změnách politiky, které ovlivňují použitelnost opatření cloudového zpracovatele, aktualizovat REG03.

11.6 [All] Top Management musí před zveřejněním schválit významné revize této politiky v REG12.

12. Související politiky

12.1 Tuto politiku podporují následující související politiky:

12.2 PII01 - Politika systému řízení informací o soukromí

12.3 PII02 - Politika rolí, odpovědností a odpovědnosti za plnění v oblasti soukromí

12.4 PII03 - Politika evidence zpracování PII a právního základu

12.5 PII06 - Politika řízení práv subjektů PII

12.6 PII07 - Politika posouzení rizik pro soukromí a DPIA

12.7 PII08 - Politika ochrany soukromí již od návrhu a ve výchozím nastavení

12.8 PII09 - Politika shromažďování, použití, zpřístupnění a sdílení PII

12.9 PII10 - Politika uchovávání, výmazu a likvidace PII

12.10 PII12 - Politika řízení ochrany soukromí u zpracovatelů, dílčích zpracovatelů a třetích stran

12.11 PII13 - Politika mezinárodního předávání PII

12.12 PII14 - Politika zabezpečení PII a řízení přístupu

12.13 PII15 - Politika řízení incidentů a porušení zabezpečení týkajících se PII

12.14 PII17 - Politika dokumentovaných informací a řízení důkazů PIMS

12.15 PII18 - Politika monitorování, auditu a zlepšování PIMS

12.16 PII20 - Politika ochrany soukromí dětí

12.17 PII21 - Politika ochrany soukromí pro AI a automatizované rozhodování

12.18 PII22 - Politika ochrany soukromí v marketingu a cookies

12.19 PII24 - Politika CCTV a fyzického monitorování

13. Referenční normy a rámce

13.1 Tato politika je mapována na následující normy a právní předpisy. Mapování vysvětluje, jak politika podporuje citované požadavky, a identifikuje interní ustanovení, která je implementují nebo podporují.

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].