					Sem vložte název registrované právnické osoby						
Číslo dokumentu: PII15					Název dokumentu: **Politika řízení incidentů týkajících se PII a porušení zabezpečení osobních údajů**						
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 7.4; Clause 7.5	Both	Supporting	Komunikace PIMS a dokumentované důkazy o porušení zabezpečení
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Operativní plánování a řízení, posouzení rizik pro soukromí a vazba na ošetření rizik
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorování, vyhodnocování, neshoda, nápravné opatření a zlepšování
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Plánování a příprava řízení incidentů pro zpracování PII
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Reakce na incidenty informační bezpečnosti zahrnující PII
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Právní, zákonné, regulační a smluvní požadavky a ochrana záznamů
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Smlouva zpracovatele se zákazníkem a podpora povinností zákazníka
GDPR	Article 5(2); Article 24	Controller	Supporting	Odpovědnost a odpovědnost správce
GDPR	Article 26	Joint Controller	Supporting	Koordinace odpovědností společných správců při porušení zabezpečení
GDPR	Article 28	Both	Supporting	Součinnost zpracovatele a

				smluvní povinnosti zpracovatele
GDPR	Article 32	Both	Supporting	Zabezpečení zpracování a schopnost detekce porušení zabezpečení
GDPR	Article 33	Both	Primary	Oznamování porušení zabezpečení osobních údajů a dokumentace porušení zabezpečení
GDPR	Article 34	Controller	Primary	Informování dotčených subjektů PII o porušení zabezpečení osobních údajů
GDPR	Article 39	Conditional	Supporting	Poradenství DPO, monitorování, spolupráce a podpora kontaktního místa
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Principy informační bezpečnosti a souladu v oblasti soukromí
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Odpovědnosti při reakci na incidenty týkající se PII a hlášení událostí
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Plánování incidentů, posouzení, reakce, získané poznatky a sběr důkazů
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Životní cyklus procesu řízení incidentů
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Politika, plán, povědomí, testování a získané poznatky k incidentům
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause	Both	Supporting	Detekce, oznamování, triáž,

	10; Clause 11; Clause 12			analýza, reakce a provozní hlášení
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Očekávání týkající se oznámení cloudového zpracovatele a záznamů o porušení zabezpečení
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Hlášení významných incidentů, je-li použitelné
DORA Regulation (EU) 2022/2554	Article 17; Article 18; Article 19	Conditional	Supporting	Řízení, klasifikace a hlášení incidentů ICT, je-li použitelné

1. Rozsah

1.1 Tato politika stanoví požadavky na identifikaci, hlášení, triáž, posouzení, zamezení šíření, oznamování, dokumentování, uzavírání a zlepšování na základě incidentů týkajících se PII a porušení zabezpečení osobních údajů v rozsahu PIMS.

1.2 Tato politika se vztahuje na:

1.2.1 organizaci jednající jako správce PII;

1.2.2 organizaci jednající jako společný správce, pokud je vyžadována koordinace odpovědností při porušení zabezpečení;

1.2.3 organizaci jednající jako zpracovatel PII;

1.2.4 organizaci jednající jako dílčí zpracovatel;

1.2.5 systémy, aplikace, služby, procesy, dodavatele, zpracovatele, dílčí zpracovatele a třetí strany, které v rozsahu PIMS zpracovávají, ukládají, přenášejí, podporují, zpřístupňují nebo jinak ovlivňují PII.

1.3 Tato politika používá REG10 - registr incidentů týkajících se PII a porušení zabezpečení osobních údajů jako primární důkazní objekt pro řízení incidentů týkajících se PII a porušení zabezpečení osobních údajů.

1.4 Tato politika používá podpůrné důkazní objekty takto:

1.4.1 REG01 pro rozsah PIMS a kontext příslušných zainteresovaných stran, právních, smluvních, odvětvových a zákaznických požadavků na hlášení.

1.4.2 REG02 pro dotčené činnosti zpracování, kategorie PII, kategorie subjektů PII, účely a systémy.

1.4.3 REG03 pro Prohlášení o použitelnosti a aktualizace použitelnosti opatření.

1.4.4 REG04 pro vazbu na rizika pro soukromí, DPIA a zbytkové riziko.

1.4.5 REG08 pro důkazy o rozhraní pro incidenty se zpracovateli, dílčími zpracovateli, zákazníky, dodavateli a třetími stranami.

1.4.6 REG09 pro vazbu na mezinárodní předávání, pokud incident ovlivňuje přeshraniční zpracování.

1.4.7 REG11 pro důkazy o školení, povědomí a způsobilosti k reakci na incidenty.

1.4.8 REG12 pro důkazy o auditu, neshodách, nápravných opatřeních a zlepšování.

1.5 Tato politika se opírá o související politiky PIMS pro specializovaná opatření:

1.5.1 PII03 upravuje evidenci činností zpracování a záznamy o právních základech.

1.5.2 PII04 upravuje oznámení o ochraně osobních údajů a opatření transparentnosti mimo komunikaci specifickou pro porušení zabezpečení.

1.5.3 PII06 upravuje žádosti subjektů PII o uplatnění práv, které vzniknou před incidentem, během incidentu nebo po něm.

1.5.4 PII07 upravuje metodiku posouzení rizik pro soukromí a DPIA.

1.5.5 PII08 upravuje opatření ochrany soukromí již od návrhu a ve výchozím nastavení.

1.5.6 PII10 upravuje opatření uchovávání, výmazu a likvidace.

1.5.7 PII12 upravuje opatření pro vztahy se zpracovateli, dílčími zpracovateli, dodavateli a třetími stranami v oblasti soukromí.

1.5.8 PII13 upravuje mechanismy mezinárodního předávání PII a záznamy o rizicích předávání.

1.5.9 PII14 upravuje preventivní a detekční opatření bezpečnosti PII a řízení přístupu.

1.5.10 PII16 upravuje školení, povědomí a způsobilost v oblasti soukromí.

1.5.11 PII17 upravuje dokumentované informace a řízení důkazů.

1.5.12 PII18 upravuje monitorování, interní audit, přezkoumání vedením, neshody, nápravná opatření a neustálé zlepšování.

1.6 Pro účely této politiky:

1.6.1 „Incident týkající se PII“ znamená podezřelou nebo potvrzenou událost, která ovlivnila, mohla ovlivnit nebo by mohla přiměřeně ovlivnit důvěrnost, integritu, dostupnost, zákonné zpracování nebo oprávněné nakládání s PII.

1.6.2 „Porušení zabezpečení osobních údajů“ znamená potvrzený incident týkající se PII zahrnující neoprávněné, nezákonné, náhodné nebo nezamýšlené zničení, ztrátu, změnu, zpřístupnění, přístup, nedostupnost nebo kompromitaci PII.

1.6.3 „Posouzení porušení zabezpečení osobních údajů“ znamená dokumentované vyhodnocení, zda je incident týkající se PII porušením zabezpečení osobních údajů, jaké PII a subjekty PII jsou dotčeny, jaká rizika mohou vzniknout, jaká oznámení nebo komunikace jsou vyžadovány a jaká nápravná opatření jsou potřebná.

1.6.4 „Vědomost“ znamená okamžik, kdy má organizace přiměřenou míru jistoty, že došlo k bezpečnostnímu incidentu nebo incidentu v oblasti soukromí a PII byly nebo mohly být kompromitovány.

1.6.5 „Incident s významným dopadem týkající se PII“ znamená incident týkající se PII zahrnující vysoce rizikové zpracování, zvláštní kategorie nebo vysoce citlivé PII, rozsáhlé PII, zranitelné osoby, regulované zákazníky, dopad ve více jurisdikcích, významný dopad na zákazníky, kompromitaci privilegovaného přístupu, veřejnou expozici, ransomware, nedostupnost služby nebo významný provozní či reputační dopad.

1.6.6 „Významná změna incidentu“ znamená nové nebo změněné informace ovlivňující rozsah incidentu, závažnost, kategorie PII, dopad na subjekty PII, rozhodnutí o oznámení, dopad na zákazníky, kořenovou příčinu, zamezení šíření, obnovu, nápravné opatření nebo povinnosti externího hlášení.

2. Účel

2.1 Účelem této politiky je zajistit, aby incidenty týkající se PII a porušení zabezpečení osobních údajů byly řešeny konzistentně, bez zbytečného odkladu, zákonně, bezpečně a s důkazy připravenými pro audit.

2.2 Tato politika podporuje odpovědnost tím, že vyžaduje zaznamenávání incidentů týkajících se PII a porušení zabezpečení osobních údajů do REG10 a jejich propojení s dotčenými záznamy o zpracování, riziky pro soukromí, vztahy se zpracovateli a dílčími zpracovateli, záznamy o předávání, nápravnými opatřeními a záznamy o školení, pokud jsou aktivovány.

2.3 Tato politika zajišťuje, že povinnosti správce, společného správce, zpracovatele a dílčího zpracovatele jsou řešeny prostřednictvím odlišných pravidel použitelnosti při zachování jednoho integrovaného modelu důkazů o incidentech a porušeních zabezpečení.

3. Cíle

3.1 Cílem této politiky je:

3.1.1 zajistit, aby podezřelé incidenty týkající se PII byly hlášeny a zaznamenávány bez zbytečného odkladu;

3.1.2 zajistit, aby incidenty týkající se PII byly tříděny a klasifikovány podle konzistentních kritérií;

3.1.3 zajistit, aby posouzení porušení zabezpečení osobních údajů zohledňovalo dotčené PII, subjekty PII, systémy, činnosti zpracování, zpracovatele, dílčí zpracovatele, předávání, rizika a nápravná opatření;

3.1.4 zajistit dokumentování rozhodnutí o oznámení správcem a komunikaci se subjekty PII;

3.1.5 zajistit, aby oznámení zpracovatele a dílčího zpracovatele o porušení zabezpečení zákazníkům nebo nadřazeným stranám byla učiněna bez zbytečného odkladu a v souladu s příslušnými smlouvami;

3.1.6 zajistit uchování a ochranu důkazů během řešení incidentu;

3.1.7 zajistit sledování zamezení šíření, eradikace, obnovy a validace prostřednictvím REG10;

3.1.8 zajistit vyhodnocení regulačních, smluvních, zákaznických a odvětvových spouštěčů hlášení, jsou-li použitelné;

3.1.9 zajistit, aby získané poznatky z incidentů vedly k nápravným opatřením a neustálému zlepšování;

3.1.10 zajistit dostupnost záznamů o incidentech a porušeních zabezpečení pro audit, přezkoumání vedením, ujištění zákazníků a regulační přezkum, je-li použitelný.

4. Prohlášení politiky

4.1 Připravenost na incidenty a příjem hlášení

4.1.1 [Both] Privacy Lead / PIMS Manager musí udržovat kritéria pro řešení incidentů týkajících se PII a porušení zabezpečení osobních údajů v REG10 alespoň jednou ročně a po každé významné změně rozsahu PIMS, právního kontextu, smluvních povinností nebo vysoce rizikového zpracování.

4.1.2 [All] Incident Response Coordinator musí zaznamenat každý nahlášený nebo zjištěný podezřelý incident týkající se PII do REG10 do jednoho pracovního dne od přijetí, nebo dříve, pokud může být aktivována použitelná lhůta pro oznámení nebo hlášení zákazníkovi.

4.1.3 [Both] System Owner / Application Owner musí uchovat relevantní systémové logy, upozornění, záznamy o přístupu, důkazy o konfiguraci a důkazy o obnově propojené s REG10, pokud podezřelý incident ovlivňuje systém nebo aplikaci zpracovávající PII.

4.1.4 [Both] Information Security Lead musí dokončit počáteční technickou triáž každé bezpečnostní události zahrnující PII do 24 hodin od detekce a zaznamenat počáteční závažnost, dotčená aktiva a stav zamezení šíření do REG10.

4.2 Klasifikace a posouzení porušení zabezpečení osobních údajů

4.2.1 [Both] Incident Response Coordinator musí klasifikovat každý záznam v REG10 jako událost bez PII, podezřelý incident týkající se PII, potvrzený incident týkající se PII nebo potvrzené porušení zabezpečení osobních údajů do 24 hodin od příjmu nebo aktualizovat záznam REG10 s důvodem, proč klasifikace zůstává nevyřízena.

4.2.2 [Both] Privacy Lead / PIMS Manager musí před dokončením rozhodnutí o oznámení porušení zabezpečení osobních údajů identifikovat dotčenou činnost zpracování, kategorie PII, kategorie subjektů PII, systémy, zpracovatele, dílčí zpracovatele, místa předávání a rizika pro soukromí v REG02, REG04, REG08, REG09 a REG10.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor musí u každého potvrzeného nebo důvodně podezřelého porušení zabezpečení osobních údajů posoudit riziko pro dotčené subjekty PII a před přijetím rozhodnutí o externím oznámení zaznamenat doporučení k oznámení, odůvodnění rizika a poradenství do REG10.

4.2.4 [Processor] Privacy Lead / PIMS Manager musí určit dotčeného správce nebo zákazníka a příslušné smluvní požadavky na oznámení, jakmile se organizace dozví o porušení zabezpečení osobních údajů ovlivňujícím PII zákazníka, a musí výsledek zaznamenat do REG08 a REG10.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager musí před jakýmkoli externím oznámením nebo komunikací společného správce ověřit dohodnutou odpovědnost za porušení

zabezpečení, odpovědnost za vedení komunikace a koordinační ujednání a musí rozhodnutí zaznamenat do REG08 a REG10.

4.2.6 [Conditional] Privacy Lead / PIMS Manager musí u každého incidentu s významným dopadem týkajícího se PII vyhodnotit použitelné právní, odvětvové, finančně-sektorové, kyberbezpečnostní, smluvní, zákaznické a na příjemce služby se vztahující spouštěče hlášení a zaznamenat výsledek použitelnosti do REG01, REG08 a REG10.

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

9. Výjimky

9.1.1 [Both] Privacy Lead / PIMS Manager musí zaznamenat jakoukoli výjimku z této politiky do REG12 před implementací, nebo do 24 hodin po nouzovém opatření, pokud předchozí schválení nebylo proveditelné.

9.1.2 [Both] Top Management musí před uzavřením incidentu schválit jakoukoli výjimku, která významně ovlivňuje načasování oznámení porušení zabezpečení, veřejnou komunikaci, závazek vůči zákazníkovi, uchování důkazů nebo riziko pro subjekt PII, přičemž důkazy o schválení musí být uchovány v REG10 a REG12.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor musí před uzavřením incidentu dokumentovat poradenství pro jakékoli opožděné oznámení, rozhodnutí o neoznámení nebo mimořádný komunikační postup, přičemž poradenství musí být uchováno v REG10.

9.1.4 [Both] Vendor / Procurement Owner musí zaznamenat výjimky řízené dodavatelem, zpracovatelem, dílčím zpracovatelem nebo zákazníkem, které ovlivňují reakci na incident, do REG08 a REG12 do pěti pracovních dnů od identifikace výjimky.

10. Uplatňování politiky

10.1.1 [All] Process Owner / Business Owner musí eskalovat selhání při hlášení podezřelého incidentu týkajícího se PII, uchování důkazů, plnění přiřazených opatření nebo spolupráci při posouzení porušení zabezpečení osobních údajů na Privacy Lead / PIMS Manager do dvou pracovních dnů od zjištění, přičemž důkazy musí být uchovány v REG12.

10.1.2 [Both] Privacy Lead / PIMS Manager musí zaznamenat neshodu REG12, pokud porušení této politiky ovlivňuje příjem hlášení incidentu, triáž, zamezení šíření, oznámení, integritu důkazů, komunikaci nebo nápravné opatření.

10.1.3 [Both] Vendor / Procurement Owner musí zahájit nápravu u dodavatele nebo zpracovatele prostřednictvím REG08 a REG12 do pěti pracovních dnů, pokud zpracovatel, dílčí zpracovatel, dodavatel nebo jiná třetí strana nesplní dohodnuté povinnosti týkající se incidentu nebo porušení zabezpečení.

10.1.4 [Both] Top Management musí při nejbližším plánovaném přezkoumání vedením přezkoumat významné nebo opakující se neshody v řízení incidentů, přičemž rozhodnutí a požadovaná opatření musí být uchována v REG12.

11. Přezkum a údržba

11.1.1 [Both] Privacy Lead / PIMS Manager musí tuto politiku přezkoumat alespoň jednou ročně a zaznamenat výsledek přezkumu, požadované změny a stav schválení do REG12.

11.1.2 [Both] Incident Response Coordinator musí do 30 kalendářních dnů po uzavření jakéhokoli incidentu s významným dopadem týkajícího se PII nebo potvrzeného porušení zabezpečení osobních údajů vyvolat poincidentní přezkum této politiky, přičemž důkazy o přezkumu musí být uchovány v REG10 a REG12.

11.1.3 [Conditional] Privacy Lead / PIMS Manager musí tuto politiku přezkoumat do 30 kalendářních dnů od okamžiku, kdy se dozví o významné změně použitelných právních,

odvětvových, zákaznických, smluvních, zpracovatelských, dílčích zpracovatelských nebo s předáváním souvisejících požadavků na hlášení incidentů, přičemž důkazy o přezkumu musí být uchovány v REG01, REG08, REG09 a REG12.

11.1.4 [Both] Internal Audit / Compliance Reviewer musí alespoň jednou ročně přezkoumat implementaci této politiky prostřednictvím programu interního auditu PIMS, přičemž auditní zjištění a nápravná opatření musí být uchována v REG12.

11.1.5 [Both] Top Management musí během plánovaného přezkoumání vedením přezkoumat trendy incidentů, významná porušení zabezpečení, výkonnost oznamování, opožděná nápravná opatření a účinnost politiky, přičemž výstupy musí být uchovány v REG12.

12. Související politiky

12.1 Tato politika se má číst společně s:

12.1.1 PII01 - Politika systému řízení informací o soukromí

12.1.2 PII02 - Politika rolí, odpovědností a odpovědnosti za ochranu soukromí

12.1.3 PII03 - Politika evidence zpracování PII a právního základu

12.1.4 PII04 - Politika oznámení o ochraně osobních údajů a transparentnosti

12.1.5 PII06 - Politika řízení práv subjektů PII

12.1.6 PII07 - Politika posouzení rizik pro soukromí a DPIA

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

12.1.8 PII10 - Politika uchovávání, výmazu a likvidace PII

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

12.1.10 PII13 - Politika mezinárodního předávání PII

12.1.11 PII14 - Politika bezpečnosti PII a řízení přístupu

12.1.12 PII16 - Politika školení, povědomí a způsobilosti v oblasti soukromí

12.1.13 PII17 - Politika dokumentovaných informací a řízení důkazů PIMS

12.1.14 PII18 - Politika monitorování, auditu a zlepšování PIMS

13. Referenční normy a rámce

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].