					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: PII15					Dokumenttitel: **Policy för hantering av personuppgiftsincidenter och PII-överträdelser**							
Version: 1.0		Ikraftträdandedatum: 01.01.2025			Dokumentägare:							
X	Policy		Standard		Rutin		Formulär		Register		Övrigt	

Revisionshistorik				
Revisionsnummer	**Revisionsdatum**	**Ändringar**	**Granskad av**	**Processägare**

Godkännanden			
Namn	**Titel**	**Datum**	**Underskrift**

Ansluten till standarder och regelverk

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	PIMS-kommunikation och dokumenterat bevismaterial för PII-överträdelser
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Koppling till operativ styrning, bedömning av integritetsrisker och riskbehandling
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Övervakning, utvärdering, avvikelse, korrigerande åtgärder och förbättring
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Planering och förberedelser för incidenthantering vid behandling av PII
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Respons på informationssäkerhetsincidenter som involverar PII
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Rättsliga, lagstadgade, regulatoriska och avtalsmässiga krav samt skydd av poster
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Stöd för biträdeskundsavtal och kundskyldigheter
GDPR	Article 5(2); Article 24	Controller	Supporting	Ansvarsskyldighet och personuppgiftsansvarigs ansvar
GDPR	Article 26	Joint Controller	Supporting	Samordning av ansvar för överträdelser mellan gemensamt personuppgiftsansvariga
GDPR	Article 28	Both	Supporting	Biträdesstöd och avtalsförpliktelser för personuppgiftsbiträde
GDPR	Article 32	Both	Supporting	Säkerhet i behandlingen och förmåga att upptäcka överträdelser
GDPR	Article 33	Both	Primary	Anmälan av personuppgiftsincidenter och dokumentation av överträdelser
GDPR	Article 34	Controller	Primary	Kommunikation om personuppgiftsincidenter till berörda registrerade

GDPR	Article 39	Conditional	Supporting	DPO-rådgivning, övervakning, samarbete och stöd som kontaktpunkt
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Principer för informationssäkerhet och efterlevnad av dataskyddskrav
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Ansvar för hantering av personuppgiftsincidenter och händelserapportering
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Incidentplanering, bedömning, respons, erfarenhetsåterföring och bevisinsamling
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Livscykel för incidenthanteringsprocessen
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Incidentpolicy, plan, medvetenhet, testning och erfarenhetsåterföring
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Drift för detektering, avisering, triage, analys, respons och rapportering
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Förväntningar på avisering och register över överträdelser för molnbaserade personuppgiftsbiträden
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Rapportering av betydande incidenter där tillämpligt
DORA Regulation (EU) 2022/2554	Article 17; Article 18; Article 19	Conditional	Supporting	Hantering, klassificering och rapportering av ICT-incidenter där tillämpligt

1. Omfattning

1.1 Denna policy definierar kraven för att identifiera, rapportera, triagera, bedöma, begränsa, anmäla, dokumentera, stänga och förbättra hanteringen utifrån personuppgiftsincidenter och PII-överträdelser inom PIMS-omfattningen.

1.2 Denna policy gäller för:

1.2.1 organisationen när den agerar som personuppgiftsansvarig för PII;

1.2.2 organisationen när den agerar som gemensamt personuppgiftsansvarig där samordning av ansvar för överträdelser krävs;

1.2.3 organisationen när den agerar som personuppgiftsbiträde för PII;

1.2.4 organisationen när den agerar som underbiträde;

1.2.5 system, applikationer, tjänster, processer, leverantörer, personuppgiftsbiträden, underbiträden och tredje parter som behandlar, lagrar, överför, stödjer, har åtkomst till eller på annat sätt påverkar PII inom PIMS-omfattningen.

1.3 Denna policy använder REG10 - PII Incident and Breach Register som primärt bevisobjekt för hantering av personuppgiftsincidenter och PII-överträdelser.

1.4 Denna policy använder stödjande bevisobjekt enligt följande:

1.4.1 REG01 för PIMS-omfattning samt tillämplig kontext för intressenter, rättsliga krav, avtal, sektorskrav och kundrapportering.

1.4.2 REG02 för berörda behandlingsaktiviteter, PII-kategorier, kategorier av registrerade, ändamål och system.

1.4.3 REG03 för tillämpbarhetsförklaring och uppdateringar av kontrolltillämplighet.

1.4.4 REG04 för koppling till integritetsrisk, DPIA och kvarstående risk.

1.4.5 REG08 för bevismaterial om incidentgränssnitt mot personuppgiftsbiträden, underbiträden, kunder, leverantörer och tredje parter.

1.4.6 REG09 för koppling till internationell överföring när en incident påverkar gränsöverskridande behandling.

1.4.7 REG11 för bevismaterial om utbildning, medvetenhet och incidenthanteringskompetens.

1.4.8 REG12 för bevismaterial om revision, avvikelse, korrigerande åtgärder och förbättring.

1.5 Denna policy bygger på relaterade PIMS-policyer för specialistkontroller:

1.5.1 PII03 styr behandlingsförteckning och register över rättslig grund.

1.5.2 PII04 styr integritetsmeddelande och transparenskontroller utanför överträdelsespecifik kommunikation.

1.5.3 PII06 styr rättighetsbegäranden från registrerade som uppstår före, under eller efter en incident.

1.5.4 PII07 styr metodik för bedömning av integritetsrisker och DPIA.

1.5.5 PII08 styr integritetsskydd genom design och dataskydd som standard.

1.5.6 PII10 styr kontroller för bevarande, radering och bortskaffning.

1.5.7 PII12 styr integritetsrelaterade relationskontroller för personuppgiftsbiträden, underbiträden, leverantörer och tredje parter.

1.5.8 PII13 styr mekanismer för internationell överföring av PII och register över överföringsrisker.

1.5.9 PII14 styr förebyggande och upptäckande säkerhets- och åtkomstkontroller för PII.

1.5.10 PII16 styr integritetsutbildning, medvetenhet och kompetens.

1.5.11 PII17 styr dokumenterad information och hantering av bevismaterial.

1.5.12 PII18 styr övervakning, internrevision, ledningens genomgång, avvikelse, korrigerande åtgärder och ständig förbättring.

1.6 I denna policy gäller följande:

1.6.1 ”Personuppgiftsincident” betyder en misstänkt eller bekräftad händelse som har påverkat, kan ha påverkat eller rimligen skulle kunna påverka konfidentialitet, riktighet, tillgänglighet, behandling med rättslig grund eller behörig hantering av PII.

1.6.2 ”PII-överträdelse” betyder en bekräftad personuppgiftsincident som innefattar obehörig, olaglig, oavsiktlig eller oavsedd förstöring, förlust, ändring, röjande av, åtkomst till, otillgänglighet för eller kompromettering av PII.

1.6.3 ”Bedömning av personuppgiftsincident” betyder den dokumenterade utvärderingen av huruvida en personuppgiftsincident är en PII-överträdelse, vilka PII och registrerade som påverkas, vilka risker som kan uppstå, vilka anmälningar eller kommunikationer som krävs och vilka avhjälpande åtgärder som behövs.

1.6.4 ”Kännedom” betyder den tidpunkt då organisationen har rimlig grad av säkerhet om att en säkerhets- eller integritetsincident har inträffat och att PII har komprometterats eller kan ha komprometterats.

1.6.5 ”Personuppgiftsincident med hög påverkan” betyder en personuppgiftsincident som innefattar högriskbehandling, särskilda kategorier av PII eller mycket känslig PII, storskalig PII, sårbara individer, reglerade kunder, påverkan i flera jurisdiktioner, väsentlig kundpåverkan, kompromettering av privilegierad åtkomst, offentlig exponering, ransomware, otillgänglighet för tjänster eller betydande operativ påverkan eller anseendepåverkan.

1.6.6 ”Väsentlig incidentförändring” betyder ny eller ändrad information som påverkar incidentens omfattning, allvarlighetsgrad, PII-kategorier, påverkan på registrerade, beslut om anmälan, kundpåverkan, rotorsak, begränsning, återhämtning, korrigerande åtgärd eller externa rapporteringsskyldigheter.

2. Syfte

2.1 Syftet med denna policy är att säkerställa att personuppgiftsincidenter och PII-överträdelser hanteras konsekvent, skyndsamt, lagenligt, säkert och med bevismaterial som har beredskap för revision.

2.2 Denna policy stödjer ansvarsskyldighet genom att kräva att personuppgiftsincidenter och PII-överträdelser registreras i REG10 och kopplas till berörda behandlingsregister, integritetsrisker, relationer med personuppgiftsbiträden och underbiträden, överföringsregister, korrigerande åtgärder och utbildningsregister när detta utlöses.

2.3 Denna policy säkerställer att skyldigheter för personuppgiftsansvarig, gemensamt personuppgiftsansvarig, personuppgiftsbiträde och underbiträde hanteras genom separata tillämplighetsregler samtidigt som en integrerad modell för bevismaterial avseende incidenter och överträdelser upprätthålls.

3. Mål

3.1 Målen med denna policy är att:

3.1.1 säkerställa att misstänkta personuppgiftsincidenter rapporteras och registreras skyndsamt;

3.1.2 säkerställa att personuppgiftsincidenter triageras och klassificeras med konsekventa kriterier;

3.1.3 säkerställa att bedömningar av personuppgiftsincidenter beaktar berörda PII, registrerade, system, behandlingsaktiviteter, personuppgiftsbiträden, underbiträden, överföringar, risker och avhjälpande åtgärder;

3.1.4 säkerställa att beslut om anmälan från personuppgiftsansvarig och kommunikation till registrerade dokumenteras;

3.1.5 säkerställa att anmälningar från personuppgiftsbiträden och underbiträden till kunder eller uppströmsparter om överträdelser görs utan onödigt dröjsmål och i enlighet med tillämpliga avtal;

3.1.6 säkerställa att bevismaterial bevaras och skyddas under incidenthantering;

3.1.7 säkerställa att begränsning, eliminering, återhämtning och validering följs upp genom REG10;

3.1.8 säkerställa att regulatoriska, avtalsmässiga, kundrelaterade och sektorsspecifika rapporteringsutlösare utvärderas där tillämpligt;

3.1.9 säkerställa att erfarenhetsåterföring från incidenter leder till korrigerande åtgärder och ständig förbättring;

3.1.10 säkerställa att incident- och överträdelseposter finns tillgängliga för revision, ledningens genomgång, kundförsäkran och regulatorisk översyn där tillämpligt.

4. Policyuttalanden

4.1 Incidentberedskap och mottagning

4.1.1 [Both] Privacy Lead / PIMS Manager MUST upprätthålla kriterier för hantering av personuppgiftsincidenter och PII-överträdelser i REG10 minst årligen och efter varje väsentlig ändring av PIMS-omfattning, rättslig kontext, avtalsförpliktelser eller högriskbehandling.

4.1.2 [All] Incident Response Coordinator MUST registrera varje rapporterad eller upptäckt misstänkt personuppgiftsincident i REG10 inom en arbetsdag från mottagandet, eller tidigare när en tillämplig tidsfrist för anmälan eller kundrapportering kan utlösas.

4.1.3 [Both] System Owner / Application Owner MUST bevara relevanta systemloggar, larm, åtkomstposter, konfigurationsunderlag och återhämtningsunderlag som är kopplade till REG10 när en misstänkt incident påverkar ett system eller en applikation som behandlar PII.

4.1.4 [Both] Information Security Lead MUST slutföra initial teknisk triage av varje säkerhetshändelse som involverar PII inom 24 timmar från detektering och registrera initial allvarlighetsgrad, berörda tillgångar och begränsningsstatus i REG10.

4.2 Klassificering och bedömning av personuppgiftsincident

4.2.1 [Both] Incident Response Coordinator MUST klassificera varje REG10-post som icke-PII-händelse, misstänkt personuppgiftsincident, bekräftad personuppgiftsincident eller bekräftad PII-överträdelse inom 24 timmar från mottagandet, eller uppdatera REG10-posten med skälet till att klassificeringen fortfarande är avvaktande.

4.2.2 [Both] Privacy Lead / PIMS Manager MUST identifiera berörd behandlingsaktivitet, PII-kategorier, kategorier av registrerade, system, personuppgiftsbiträden, underbiträden, överföringsplatser och integritetsrisker i REG02, REG04, REG08, REG09 och REG10 innan beslutet om anmälan av överträdelse slutligt fastställs.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor MUST bedöma risken för berörda registrerade för varje bekräftad eller rimligen misstänkt PII-överträdelse och registrera rekommendation om anmälan, riskmotivering och rådgivning i REG10 innan beslut om extern anmälan fattas.

4.2.4 [Processor] Privacy Lead / PIMS Manager MUST identifiera berörd personuppgiftsansvarig eller kund och tillämpliga avtalskrav för anmälan så snart organisationen får kännedom om en PII-överträdelse som påverkar kundens PII, och MUST registrera utfallet i REG08 och REG10.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager MUST verifiera överenskommet ansvar för överträdelsen, huvudansvar för kommunikation och samordningsarrangemang innan extern

anmälan eller kommunikation görs av en gemensamt personuppgiftsansvarig, och MUST registrera beslutet i REG08 och REG10.

4.2.6 [Conditional] Privacy Lead / PIMS Manager MUST utvärdera tillämpliga rapporteringsutlösare enligt lag, sektor, finanssektor, cybersäkerhet, avtal, kundkrav och tjänstemottagarkrav för varje personuppgiftsincident med hög påverkan och registrera utfallet av tillämpligheten i REG01, REG08 och REG10.

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Undantag

9.1.1 [Both] Privacy Lead / PIMS Manager MUST registrera varje undantag från denna policy i REG12 före genomförande, eller inom 24 timmar efter nödåtgärd när förhandsgodkännande inte var genomförbart.

9.1.2 [Both] Top Management MUST godkänna varje undantag som väsentligt påverkar tidsfrister för anmälan av överträdelse, offentlig kommunikation, kundåtagande, bevarande av bevismaterial eller risk för registrerade innan incidenten stängs, med godkännandeunderlag bevarat i REG10 och REG12.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor MUST dokumentera rådgivning för varje fördröjd anmälan, beslut om utebliven anmälan eller exceptionellt kommunikationssätt före incidentstängning, med rådgivningen bevarad i REG10.

9.1.4 [Both] Vendor / Procurement Owner MUST registrera leverantörs-, personuppgiftsbiträdes-, underbiträdes- eller kunddrivna undantag som påverkar incidentrespons i REG08 och REG12 inom fem arbetsdagar från att undantaget identifierades.

10. Efterlevnad och tillämpning

10.1.1 [All] Process Owner / Business Owner MUST eskalera underlåtenhet att rapportera en misstänkt personuppgiftsincident, bevara bevismaterial, följa tilldelade åtgärder eller samarbeta vid bedömning av personuppgiftsincident till Privacy Lead / PIMS Manager inom två arbetsdagar från upptäckt, med bevismaterial bevarat i REG12.

10.1.2 [Both] Privacy Lead / PIMS Manager MUST registrera en REG12-avvikelse när en överträdelse av denna policy påverkar incidentmottagning, triage, begränsning, anmälan, bevisintegritet, kommunikation eller korrigerande åtgärd.

10.1.3 [Both] Vendor / Procurement Owner MUST initiera åtgärder gentemot leverantör eller personuppgiftsbiträde genom REG08 och REG12 inom fem arbetsdagar när ett personuppgiftsbiträde, underbiträde, en leverantör eller annan tredje part inte uppfyller överenskomna incident- eller överträdelseskyldigheter.

10.1.4 [Both] Top Management MUST granska väsentliga eller återkommande avvikelser i incidenthantering vid nästa planerade ledningsgenomgång, med beslut och nödvändiga åtgärder bevarade i REG12.

11. Granskning och underhåll

11.1.1 [Both] Privacy Lead / PIMS Manager MUST granska denna policy minst årligen och registrera granskningsutfall, nödvändiga ändringar och godkännandestatus i REG12.

11.1.2 [Both] Incident Response Coordinator MUST initiera en efterincidentgranskning av denna policy inom 30 kalenderdagar efter stängning av varje personuppgiftsincident med hög påverkan eller bekräftad PII-överträdelse, med granskningsunderlag bevarat i REG10 och REG12.

11.1.3 [Conditional] Privacy Lead / PIMS Manager MUST granska denna policy inom 30 kalenderdagar från att ha fått kännedom om en väsentlig ändring av tillämpliga rättsliga,

sektorsspecifika, kundrelaterade, avtalsmässiga, personuppgiftsbiträdes-, underbiträdes- eller överföringsrelaterade incidentrapporteringskrav, med granskningsunderlag bevarat i REG01, REG08, REG09 och REG12.

11.1.4 [Both] Internal Audit / Compliance Reviewer MUST granska genomförandet av denna policy minst årligen genom PIMS internrevisionsprogram, med revisionsiakttagelser och korrigerande åtgärder bevarade i REG12.

11.1.5 [Both] Top Management MUST granska incidenttrender, betydande överträdelser, anmälningsprestation, försenade korrigerande åtgärder och policyens effektivitet under planerad ledningsgenomgång, med resultat bevarade i REG12.

12. Relaterade policyer

12.1 Denna policy bör läsas tillsammans med:

12.1.1 PII01 - Policy för ledningssystem för hantering av integritetsinformation

12.1.2 PII02 - Policy för integritetsroller, ansvar och ansvarsskyldighet

12.1.3 PII03 - Policy för behandlingsförteckning för PII och rättslig grund

12.1.4 PII04 - Policy för integritetsmeddelande och transparens

12.1.5 PII06 - Policy för hantering av rättigheter för registrerade

12.1.6 PII07 - Policy för bedömning av integritetsrisker och DPIA

12.1.7 PII08 - Policy för integritetsskydd genom design och dataskydd som standard

12.1.8 PII10 - Policy för bevarande, radering och bortskaffning av PII

12.1.9 PII12 - Policy för integritetshantering av personuppgiftsbiträden, underbiträden och tredje parter

12.1.10 PII13 - Policy för internationell överföring av PII

12.1.11 PII14 - Policy för säkerhet och åtkomstkontroll för PII

12.1.12 PII16 - Policy för integritetsutbildning, medvetenhet och kompetens

12.1.13 PII17 - Policy för PIMS-dokumenterad information och bevismaterialhantering

12.1.14 PII18 - Policy för PIMS-övervakning, revision och förbättring

13. Referensstandarder och ramverk

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].