					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: PII15					Dokumenttitel: **Politik for håndtering af PII-hændelser og brud på persondatasikkerheden**						
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:						
X	Politik		Standard		Procedure		Formular		Register		Andet

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

Tilpasset relevante standarder og regler

Standard / regulering	Klausul / kontrol / artikel	Anvendelighed	Dækningstype	Kommentar
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	PIMS-kommunikation og dokumenteret bevismateriale for brud
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Operationel styring, risikovurdering vedrørende databeskyttelse og kobling til risikobehandling
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Overvågning, evaluering, afvigelse, korrigerende handling og forbedring
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Planlægning og forberedelse af hændelsesstyring for behandling af PII
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Respons på informationssikkerhedshændelser, der involverer PII
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Retlige, lovbestemte, regulatoriske og kontraktlige krav samt beskyttelse af registreringer
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Databehandlers kundeaftale og understøttelse af kundens forpligtelser
GDPR	Article 5(2); Article 24	Controller	Supporting	Ansvarlighed og dataansvarliges ansvar
GDPR	Article 26	Joint Controller	Supporting	Koordinering af fælles dataansvarliges ansvar ved brud
GDPR	Article 28	Both	Supporting	Databehandlerbistand og databehandlers kontraktlige forpligtelser
GDPR	Article 32	Both	Supporting	Behandlingssikkerhed og kapacitet til detektion af brud
GDPR	Article 33	Both	Primary	Underretning om brud på persondatasikkerheden og dokumentation af brud
GDPR	Article 34	Controller	Primary	Kommunikation om brud på persondatasikkerheden til berørte registrerede
GDPR	Article 39	Conditional	Supporting	DPO-rådgivning, overvågning, samarbejde og understøttelse af kontaktpunkt

ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Principper for informationssikkerhed og efterlevelse af databeskyttelse
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Ansvar for respons på PII-hændelser og rapportering af hændelser
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Hændelsesplanlægning, vurdering, respons, læring og indsamling af bevismateriale
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Proceslivscyklus for hændelsesstyring
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Hændelsespolitik, plan, bevidstgørelse, test og læring
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Detektion, underretning, triage, analyse, respons og rapporteringsaktiviteter
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Forventninger til cloud-databehandlers underretning og registrering af brud
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Rapportering af væsentlige hændelser, hvor det er relevant
DORA Regulation (EU) 2022/2554	Article 17; Article 18; Article 19	Conditional	Supporting	Håndtering, klassificering og rapportering af ICT-hændelser, hvor det er relevant

1. Omfang

1.1 Denne politik fastlægger kravene til at identificere, rapportere, triagere, vurdere, inddæmme, underrette om, dokumentere, lukke og forbedre på baggrund af PII-hændelser og brud på persondatasikkerheden inden for PIMS-omfanget.

1.2 Denne politik gælder for:

1.2.1 organisationen, når den handler som dataansvarlig for PII;

1.2.2 organisationen, når den handler som fælles dataansvarlig, hvor koordinering af ansvar ved brud er påkrævet;

1.2.3 organisationen, når den handler som databehandler for PII;

1.2.4 organisationen, når den handler som underdatabehandler;

1.2.5 systemer, applikationer, tjenester, processer, leverandører, databehandlere, underdatabehandlere og tredjeparter, der behandler, lagrer, transmitterer, understøtter, tilgår eller på anden måde påvirker PII inden for PIMS-omfanget.

1.3 Denne politik anvender REG10 - register over PII-hændelser og brud på persondatasikkerheden som det primære bevisobjekt for håndtering af PII-hændelser og brud på persondatasikkerheden.

1.4 Denne politik anvender understøttende bevisobjekter som følger:

1.4.1 REG01 for PIMS-omfang, relevante interessenter samt retlig, kontraktlig, sektorbestemt og kundemæssig rapporteringskontekst.

1.4.2 REG02 for berørte behandlingsaktiviteter, PII-kategorier, kategorier af registrerede, formål og systemer.

1.4.3 REG03 for Anvendelseserklæring og opdateringer af kontrolanvendelighed.

1.4.4 REG04 for kobling til databeskyttelsesrisiko, DPIA og restrisiko.

1.4.5 REG08 for bevismateriale om hændelsesgrænseflader med databehandlere, underdatabehandlere, kunder, leverandører og tredjeparter.

1.4.6 REG09 for kobling til internationale overførsler, når en hændelse påvirker grænseoverskridende behandling.

1.4.7 REG11 for bevismateriale om træning, bevidstgørelse og kompetence til hændelseshåndtering.

1.4.8 REG12 for bevismateriale om revision, afvigelse, korrigerende handling og forbedring.

1.5 Denne politik bygger på relaterede PIMS-politikker for specialistkontroller:

1.5.1 PII03 regulerer fortegnelse over behandlingsaktiviteter og registreringer af behandlingsgrundlag.

1.5.2 PII04 regulerer privatlivsmeddelelse og gennemsigtighedskontroller uden for brudspecifik kommunikation.

1.5.3 PII06 regulerer rettighedsanmodninger fra registrerede, der opstår før, under eller efter en hændelse.

1.5.4 PII07 regulerer metode for risikovurdering vedrørende databeskyttelse og DPIA.

1.5.5 PII08 regulerer kontroller for databeskyttelse gennem design og standardindstillinger.

1.5.6 PII10 regulerer kontroller for opbevaring, sletning og bortskaffelse.

1.5.7 PII12 regulerer kontroller for databeskyttelsesrelationer med databehandlere, underdatabehandlere, leverandører og tredjeparter.

1.5.8 PII13 regulerer overførselsgrundlag for international overførsel af PII og registreringer af overførselsrisici.

1.5.9 PII14 regulerer forebyggende og opdagende PII-sikkerheds- og adgangskontroller.

1.5.10 PII16 regulerer træning, bevidstgørelse og kompetence vedrørende databeskyttelse.

1.5.11 PII17 regulerer dokumenteret information og styring af bevismateriale.

1.5.12 PII18 regulerer overvågning, intern revision, ledelsens gennemgang, afvigelse, korrigerende handling og løbende forbedring.

1.6 I denne politik:

1.6.1 "PII-hændelse" betyder en mistænkt eller bekræftet hændelse, der har påvirket, kan have påvirket eller med rimelighed kunne påvirke fortrolighed, integritet, tilgængelighed, lovlig behandling eller autoriseret håndtering af PII.

1.6.2 "Brud på persondatasikkerheden" betyder en bekræftet PII-hændelse, der involverer uautoriseret, ulovlig, hændelig eller utilsigtet tilintetgørelse, tab, ændring, videregivelse af, adgang til, utilgængelighed af eller kompromittering af PII.

1.6.3 "Vurdering af brud" betyder den dokumenterede evaluering af, om en PII-hændelse er et brud på persondatasikkerheden, hvilke PII og registrerede der er berørt, hvilke risici der kan opstå, hvilke underretninger eller kommunikationer der kræves, og hvilke afhjælpende handlinger der er nødvendige.

1.6.4 "Kendskab" betyder det tidspunkt, hvor organisationen har en rimelig grad af sikkerhed for, at en sikkerheds- eller databeskyttelseshændelse er indtruffet, og at PII er eller kan være blevet kompromitteret.

1.6.5 "PII-hændelse med højt konsekvensniveau" betyder en PII-hændelse, der involverer højrisikobehandling, særlige kategorier af personoplysninger eller meget følsomme PII, PII i stor skala, sårbare personer, regulerede kunder, påvirkning på tværs af jurisdiktioner, væsentlig kundepåvirkning, kompromittering af privilegeret adgang, offentlig eksponering, ransomware, utilgængelighed af tjenester eller væsentlig driftsmæssig eller omdømmemæssig påvirkning.

1.6.6 "Væsentlig ændring i hændelsesoplysninger" betyder nye eller ændrede oplysninger, der påvirker hændelsens omfang, alvorlighed, PII-kategorier, påvirkning på registrerede, beslutning om anmeldelse/underretning ved brud, kundepåvirkning, rodårsag, inddæmning, genopretning, korrigerende handling eller eksterne rapporteringsforpligtelser.

2. Formål

2.1 Formålet med denne politik er at sikre, at PII-hændelser og brud på persondatasikkerheden håndteres ensartet, rettidigt, lovligt, sikkert og med revisionsklart bevismateriale.

2.2 Denne politik understøtter ansvarlighed ved at kræve, at PII-hændelser og brud på persondatasikkerheden registreres i REG10 og kobles til berørte behandlingsregistreringer, databeskyttelsesrisici, databehandler- og underdatabehandlerforhold, overførselsregistreringer, korrigerende handlinger og træningsregistreringer, hvor dette udløses.

2.3 Denne politik sikrer, at forpligtelser for dataansvarlige, fælles dataansvarlige, databehandlere og underdatabehandlere håndteres gennem særskilte anvendelighedsregler, samtidig med at én integreret model for bevismateriale om hændelser og brud opretholdes.

3. Mål

3.1 Målene med denne politik er at:

3.1.1 sikre, at mistænkte PII-hændelser rapporteres og registreres rettidigt;

3.1.2 sikre, at PII-hændelser triageres og klassificeres efter ensartede kriterier;

3.1.3 sikre, at vurderinger af brud omfatter berørte PII, registrerede, systemer, behandlingsaktiviteter, databehandlere, underdatabehandlere, overførsler, risici og afhjælpende handlinger;

3.1.4 sikre, at beslutninger om underretning fra dataansvarlig og kommunikation til registrerede dokumenteres;

3.1.5 sikre, at databehandleres og underdatabehandleres underretninger om brud til kunder eller forudgående parter sker uden unødig forsinkelse og i overensstemmelse med gældende aftaler;

3.1.6 sikre, at bevismateriale bevares og beskyttes under hændelseshåndtering;

3.1.7 sikre, at inddæmning, fjernelse, genopretning og validering spores gennem REG10;

3.1.8 sikre, at udløsende forhold for regulatorisk, kontraktlig, kunde- og sektorbestemt rapportering vurderes, hvor det er relevant;

3.1.9 sikre, at læring fra hændelser resulterer i korrigerende handling og løbende forbedring;

3.1.10 sikre, at registreringer af hændelser og brud er tilgængelige for revision, ledelsens gennemgang, kundedokumentation og regulatorisk gennemgang, hvor det er relevant.

4. Politikudsagn

4.1 Hændelsesberedskab og modtagelse

4.1.1 [Both] Privacy Lead / PIMS Manager SKAL vedligeholde kriterier for håndtering af PII-hændelser og brud på persondatasikkerheden i REG10 mindst årligt og efter enhver væsentlig ændring af PIMS-omfang, retlig kontekst, kontraktlige forpligtelser eller højrisikobehandling.

4.1.2 [All] Incident Response Coordinator SKAL registrere enhver rapporteret eller detekteret mistænkt PII-hændelse i REG10 inden for én arbejdsdag efter modtagelse, eller tidligere hvis en gældende underretningsfrist eller kunderapporteringsfrist kan blive udløst.

4.1.3 [Both] System Owner / Application Owner SKAL bevare relevante systemlogfiler, alarmer, adgangsregistreringer, konfigurationsbevismateriale og genopretningsbevismateriale, der er knyttet til REG10, når en mistænkt hændelse påvirker et system eller en applikation, der behandler PII.

4.1.4 [Both] Information Security Lead SKAL gennemføre indledende teknisk triage af enhver sikkerhedshændelse, der involverer PII, inden for 24 timer efter detektion og registrere den indledende alvorlighed, berørte aktiver og inddæmningsstatus i REG10.

4.2 Klassificering og vurdering af brud

4.2.1 [Both] Incident Response Coordinator SKAL klassificere hver REG10-post som en ikke-PII-hændelse, mistænkt PII-hændelse, bekræftet PII-hændelse eller bekræftet brud på persondatasikkerheden inden for 24 timer efter modtagelse eller opdatere REG10-registreringen med årsagen til, at klassificeringen fortsat afventer.

4.2.2 [Both] Privacy Lead / PIMS Manager SKAL identificere den berørte behandlingsaktivitet, PII-kategorier, kategorier af registrerede, systemer, databehandlere, underdatabehandlere, overførselslokationer og databeskyttelsesrisici i REG02, REG04, REG08, REG09 og REG10, før beslutningen om anmeldelse/underretning ved brud færdiggøres.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor SKAL vurdere risikoen for berørte registrerede for hvert bekræftet eller rimeligt mistænkt brud på persondatasikkerheden og registrere underretningsanbefaling, risikobegrundelse og rådgivning i REG10, før beslutningen om ekstern underretning træffes.

4.2.4 [Processor] Privacy Lead / PIMS Manager SKAL identificere den berørte dataansvarlige eller kunde og relevante kontraktlige underretningskrav, så snart organisationen bliver bekendt med et brud på persondatasikkerheden, der påvirker kundens PII, og SKAL registrere resultatet i REG08 og REG10.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager SKAL verificere det aftalte ansvar ved brud, hovedansvaret for kommunikation og koordineringsordningen før enhver ekstern underretning eller kommunikation fra en fælles dataansvarlig, og SKAL registrere beslutningen i REG08 og REG10.

4.2.6 [Conditional] Privacy Lead / PIMS Manager SKAL vurdere relevante udløsende forhold for retlig, sektorbestemt, finanssektorrelateret, cybersikkerhedsrelateret, kontraktlig, kundemæssig og tjenestemodtagerrelateret rapportering for hver PII-hændelse med højt konsekvensniveau og registrere anvendelighedsresultatet i REG01, REG08 og REG10.

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Undtagelser

9.1.1 [Both] Privacy Lead / PIMS Manager SKAL registrere enhver undtagelse fra denne politik i REG12 før implementering eller inden for 24 timer efter nødhandling, hvor forudgående godkendelse ikke var mulig.

9.1.2 [Both] Top Management SKAL godkende enhver undtagelse, der væsentligt påvirker timing for underretning ved brud, offentlig kommunikation, kundeforpligtelse, bevaring af bevismateriale eller risiko for registrerede, før hændelsen lukkes, med godkendelsesbevismateriale opbevaret i REG10 og REG12.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor SKAL dokumentere rådgivning for enhver forsinket underretning, beslutning om manglende underretning eller ekstraordinær kommunikationsmetode før hændelseslukning, med rådgivning opbevaret i REG10.

9.1.4 [Both] Vendor / Procurement Owner SKAL registrere leverandør-, databehandler-, underdatabehandler- eller kundedrevne undtagelser, der påvirker hændelsesrespons, i REG08 og REG12 inden for fem arbejdsdage efter identifikation af undtagelsen.

10. Håndhævelse

10.1.1 [All] Process Owner / Business Owner SKAL eskalere manglende rapportering af en mistænkt PII-hændelse, manglende bevaring af bevismateriale, manglende overholdelse af tildelte handlinger eller manglende samarbejde om vurdering af brud til Privacy Lead / PIMS Manager inden for to arbejdsdage efter opdagelse, med bevismateriale opbevaret i REG12.

10.1.2 [Both] Privacy Lead / PIMS Manager SKAL registrere en REG12-afvigelse, når et brud på denne politik påvirker hændelsesmodtagelse, triage, inddæmning, underretning, bevismaterialets integritet, kommunikation eller korrigerende handling.

10.1.3 [Both] Vendor / Procurement Owner SKAL igangsætte afhjælpning hos leverandør eller databehandler gennem REG08 og REG12 inden for fem arbejdsdage, når en databehandler, underdatabehandler, leverandør eller anden tredjepart ikke opfylder aftalte hændelses- eller brudforpligtelser.

10.1.4 [Both] Top Management SKAL gennemgå væsentlige eller tilbagevendende afvigelser i hændelsesstyringen ved den næste planlagte ledelsesgennemgang, med beslutninger og påkrævede handlinger opbevaret i REG12.

11. Gennemgang og vedligeholdelse

11.1.1 [Both] Privacy Lead / PIMS Manager SKAL gennemgå denne politik mindst årligt og registrere gennemgangsresultat, krævede ændringer og godkendelsesstatus i REG12.

11.1.2 [Both] Incident Response Coordinator SKAL udløse en efterhændelsesgennemgang af denne politik inden for 30 kalenderdage efter lukning af enhver PII-hændelse med højt konsekvensniveau eller ethvert bekræftet brud på persondatasikkerheden, med gennemgangsbevismateriale opbevaret i REG10 og REG12.

11.1.3 [Conditional] Privacy Lead / PIMS Manager SKAL gennemgå denne politik inden for 30 kalenderdage efter at være blevet bekendt med en væsentlig ændring af relevante retlige, sektorbestemte, kunde-, kontraktlige, databehandler-, underdatabehandler- eller

overførselsrelaterede krav til hændelsesrapportering, med gennemgangsbevismateriale opbevaret i REG01, REG08, REG09 og REG12.

11.1.4 [Both] Internal Audit / Compliance Reviewer SKAL gennemgå implementeringen af denne politik mindst årligt gennem PIMS' interne revisionsprogram, med revisionskonstateringer og korrigerende handlinger opbevaret i REG12.

11.1.5 [Both] Top Management SKAL gennemgå hændelsestendenser, væsentlige brud, underretningsperformance, forfaldne korrigerende handlinger og politikkens effektivitet under planlagt ledelsesgennemgang, med output opbevaret i REG12.

12. Relaterede politikker

12.1 Denne politik bør læses sammen med:

12.1.1 PII01 - Politik for ledelsessystem for databeskyttelsesoplysninger

12.1.2 PII02 - Politik for databeskyttelsesroller, ansvar og ansvarlighed

12.1.3 PII03 - Politik for fortegnelse over PII-behandling og behandlingsgrundlag

12.1.4 PII04 - Politik for privatlivsmeddelelse og gennemsigtighed

12.1.5 PII06 - Politik for håndtering af registreredes rettigheder

12.1.6 PII07 - Politik for risikovurdering vedrørende databeskyttelse og DPIA

12.1.7 PII08 - Politik for databeskyttelse gennem design og standardindstillinger

12.1.8 PII10 - Politik for opbevaring, sletning og bortskaffelse af PII

12.1.9 PII12 - Politik for databeskyttelsesstyring af databehandlere, underdatabehandlere og tredjeparter

12.1.10 PII13 - Politik for international overførsel af PII

12.1.11 PII14 - Politik for PII-sikkerhed og adgangsstyring

12.1.12 PII16 - Politik for træning, bevidstgørelse og kompetence vedrørende databeskyttelse

12.1.13 PII17 - Politik for PIMS-dokumenteret information og styring af bevismateriale

12.1.14 PII18 - Politik for PIMS-overvågning, revision og forbedring

13. Referencestandarder og rammeværker

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].