					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: PII15					Titolo del documento: **Politica di gestione degli incidenti relativi ai dati personali e delle violazioni dei dati personali**							
Versione: 1.0		Data di entrata in vigore: 01.01.2025			Proprietario del documento:							
X	Politica		Standard		Procedura		Modulo		Registro		Altro	

Cronologia delle revisioni				
Numero di revisione	**Data di revisione**	**Modifiche**	**Riesaminato da**	**Proprietario del processo**

Approvazioni			
Nome	**Ruolo**	**Data**	**Firma**

Allineamento a standard e normative applicabili

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Comunicazioni PIMS ed evidenze documentate delle violazioni
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Collegamento tra controllo operativo, valutazione del rischio privacy e trattamento del rischio
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitoraggio, valutazione, non conformità, azione correttiva e miglioramento
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Pianificazione e preparazione della gestione degli incidenti per il trattamento di PII
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Risposta agli incidenti di sicurezza delle informazioni che coinvolgono PII
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Requisiti legali, statutari, normativi, contrattuali e protezione delle registrazioni
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Accordo del responsabile del trattamento con il cliente e supporto agli obblighi del cliente
GDPR	Article 5(2); Article 24	Controller	Supporting	Responsabilizzazione e responsabilità del titolare del trattamento
GDPR	Article 26	Joint Controller	Supporting	Coordinamento delle responsabilità dei contitolari del trattamento in caso di violazione

GDPR	Article 28	Both	Supporting	Assistenza del responsabile del trattamento e obblighi contrattuali del responsabile del trattamento
GDPR	Article 32	Both	Supporting	Sicurezza del trattamento e capacità di rilevazione delle violazioni
GDPR	Article 33	Both	Primary	Notifica delle violazioni dei dati personali e documentazione delle violazioni
GDPR	Article 34	Controller	Primary	Comunicazione delle violazioni dei dati personali agli interessati coinvolti
GDPR	Article 39	Conditional	Supporting	Consulenza del DPO, monitoraggio, cooperazione e supporto come punto di contatto
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Principi di sicurezza delle informazioni e conformità privacy
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Responsabilità di risposta agli incidenti relativi ai dati personali e segnalazione degli eventi
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Pianificazione degli incidenti, valutazione, risposta, lezioni apprese e raccolta delle evidenze
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Ciclo di vita del processo di gestione degli incidenti
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Politica, piano, sensibilizzazione, test e lezioni apprese relativi agli incidenti

ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Operazioni di rilevazione, notifica, triage, analisi, risposta e segnalazione
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Aspettative di notifica e registrazione delle violazioni per i responsabili del trattamento in cloud
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Segnalazione degli incidenti significativi ove applicabile
DORA Regulation (EU) 2022/2554	Article 17; Article 18; Article 19	Conditional	Supporting	Gestione, classificazione e segnalazione degli incidenti ICT ove applicabile

1. Ambito di applicazione

1.1 La presente politica definisce i requisiti per identificare, segnalare, sottoporre a triage, valutare, contenere, notificare, documentare, chiudere e migliorare sulla base degli incidenti relativi ai dati personali e delle violazioni dei dati personali nell'ambito di applicazione del PIMS.

1.2 La presente politica si applica a:

1.2.1 l'organizzazione che agisce in qualità di titolare del trattamento di PII;

1.2.2 l'organizzazione che agisce in qualità di contitolare del trattamento quando è richiesto il coordinamento delle responsabilità in caso di violazione;

1.2.3 l'organizzazione che agisce in qualità di responsabile del trattamento di PII;

1.2.4 l'organizzazione che agisce in qualità di sub-responsabile;

1.2.5 sistemi, applicazioni, servizi, processi, fornitori, responsabili del trattamento, sub-responsabili e terze parti che trattano, archiviano, trasmettono, supportano, accedono a PII o altrimenti incidono su PII nell'ambito di applicazione del PIMS.

1.3 La presente politica utilizza REG10 - Registro degli incidenti relativi ai dati personali e delle violazioni dei dati personali come principale oggetto di evidenza per la gestione degli incidenti relativi ai dati personali e delle violazioni dei dati personali.

1.4 La presente politica utilizza gli oggetti di evidenza di supporto come segue:

1.4.1 REG01 per l'ambito di applicazione del PIMS e per il contesto relativo a parti interessate applicabili, requisiti legali, contrattuali, settoriali e di segnalazione al cliente.

1.4.2 REG02 per le attività di trattamento interessate, le categorie di PII, le categorie di interessati, le finalità e i sistemi.

1.4.3 REG03 per la Dichiarazione di Applicabilità e gli aggiornamenti dell'applicabilità dei controlli.

1.4.4 REG04 per il collegamento con rischio privacy, DPIA e rischio residuo.

1.4.5 REG08 per le evidenze relative all'interfaccia sugli incidenti con responsabili del trattamento, sub-responsabili, clienti, fornitori e terze parti.

1.4.6 REG09 per il collegamento con i trasferimenti internazionali quando un incidente interessa un trattamento transfrontaliero.

1.4.7 REG11 per le evidenze di formazione, sensibilizzazione e competenza nella risposta agli incidenti.

1.4.8 REG12 per le evidenze di audit, non conformità, azione correttiva e miglioramento.

1.5 La presente politica si basa sulle politiche PIMS correlate per i controlli specialistici:

1.5.1 PII03 disciplina l'inventario dei trattamenti e le registrazioni della base giuridica.

1.5.2 PII04 disciplina l'informativa privacy e i controlli di trasparenza al di fuori delle comunicazioni specifiche relative alle violazioni.

1.5.3 PII06 disciplina le richieste di esercizio dei diritti degli interessati che sorgono prima, durante o dopo un incidente.

1.5.4 PII07 disciplina la valutazione del rischio privacy e la metodologia DPIA.

1.5.5 PII08 disciplina i controlli di privacy by design e privacy by default.

1.5.6 PII10 disciplina i controlli di conservazione, cancellazione e smaltimento.

1.5.7 PII12 disciplina i controlli dei rapporti privacy con responsabili del trattamento, sub-responsabili, fornitori e terze parti.

1.5.8 PII13 disciplina gli strumenti di trasferimento internazionale di PII e le registrazioni del rischio di trasferimento.

1.5.9 PII14 disciplina i controlli preventivi e di rilevamento per la sicurezza e l'accesso alle PII.

1.5.10 PII16 disciplina la formazione, la sensibilizzazione e la competenza in materia di privacy.

1.5.11 PII17 disciplina la gestione delle informazioni documentate e delle evidenze.

1.5.12 PII18 disciplina monitoraggio, audit interno, riesame della direzione, non conformità, azione correttiva e miglioramento continuo.

1.6 Ai fini della presente politica:

1.6.1 “Incidente relativo ai dati personali” indica un evento sospetto o confermato che ha inciso, può avere inciso o potrebbe ragionevolmente incidere sulla riservatezza, integrità, disponibilità, liceità del trattamento o gestione autorizzata di PII.

1.6.2 “Violazione dei dati personali” indica un incidente relativo ai dati personali confermato che comporta distruzione, perdita, alterazione, divulgazione, accesso, indisponibilità o compromissione di PII, non autorizzati, illeciti, accidentali o non intenzionali.

1.6.3 “Valutazione della violazione” indica la valutazione documentata volta a stabilire se un incidente relativo ai dati personali costituisce una violazione dei dati personali, quali PII e interessati sono coinvolti, quali rischi possono derivarne, quali notifiche o comunicazioni sono richieste e quali azioni di rimedio sono necessarie.

1.6.4 “Presa di conoscenza” indica il momento in cui l’organizzazione dispone di un ragionevole grado di certezza che si sia verificato un incidente di sicurezza o privacy e che PII siano state o possano essere state compromesse.

1.6.5 “Incidente relativo ai dati personali ad alto impatto” indica un incidente relativo ai dati personali che coinvolge trattamenti ad alto rischio, categorie particolari o PII altamente sensibili, PII su larga scala, persone vulnerabili, clienti regolamentati, impatti multi-giurisdizionali, impatti rilevanti sui clienti, compromissione di accessi privilegiati, esposizione pubblica, ransomware, indisponibilità del servizio o impatti operativi o reputazionali significativi.

1.6.6 “Modifica sostanziale dell’incidente” indica informazioni nuove o modificate che incidono su ambito, gravità, categorie di PII, impatto sugli interessati, decisione di notifica, impatto sui clienti, causa radice, contenimento, ripristino, azione correttiva o obblighi di segnalazione esterna relativi all’incidente.

2. Finalità

2.1 La finalità della presente politica è assicurare che gli incidenti relativi ai dati personali e le violazioni dei dati personali siano gestiti in modo coerente, tempestivo, lecito, sicuro e con evidenze idonee a dimostrare la conformità in sede di audit.

2.2 La presente politica supporta la responsabilizzazione richiedendo che gli incidenti relativi ai dati personali e le violazioni dei dati personali siano registrati in REG10 e collegati alle registrazioni dei trattamenti interessati, ai rischi privacy, ai rapporti con responsabili e sub-responsabili del trattamento, alle registrazioni dei trasferimenti, alle azioni correttive e alle registrazioni della formazione, ove attivati.

2.3 La presente politica assicura che gli obblighi di titolare del trattamento, contitolare del trattamento, responsabile del trattamento e sub-responsabile siano gestiti mediante regole di applicabilità distinte, mantenendo al contempo un unico modello integrato di evidenze per incidenti e violazioni.

3. Obiettivi

3.1 Gli obiettivi della presente politica sono:

3.1.1 assicurare che gli incidenti relativi ai dati personali sospetti siano segnalati e registrati tempestivamente;

3.1.2 assicurare che gli incidenti relativi ai dati personali siano sottoposti a triage e classificati secondo criteri coerenti;

3.1.3 assicurare che le valutazioni delle violazioni considerino PII, interessati, sistemi, attività di trattamento, responsabili del trattamento, sub-responsabili, trasferimenti, rischi e azioni di rimedio interessati;

3.1.4 assicurare che le decisioni di notifica del titolare del trattamento e di comunicazione agli interessati siano documentate;

3.1.5 assicurare che le notifiche di violazione da parte di responsabili del trattamento e sub-responsabili a clienti o soggetti a monte siano effettuate senza ingiustificato ritardo e in conformità agli accordi applicabili;

3.1.6 assicurare che le evidenze siano conservate e protette durante la gestione dell'incidente;

3.1.7 assicurare che contenimento, eradicazione, ripristino e validazione siano tracciati tramite REG10;

3.1.8 assicurare che, ove applicabile, siano valutati i trigger di segnalazione regolamentari, contrattuali, verso clienti e settoriali;

3.1.9 assicurare che le lezioni apprese dagli incidenti producano azioni correttive e miglioramento continuo;

3.1.10 assicurare che le registrazioni degli incidenti e delle violazioni siano disponibili per audit, riesame della direzione, assurance dei clienti e riesame normativo ove applicabile.

4. Dichiarazioni della politica

4.1 Preparazione e acquisizione degli incidenti

4.1.1 [Both] Il Privacy Lead / PIMS Manager DEVE mantenere i criteri di gestione degli incidenti relativi ai dati personali e delle violazioni dei dati personali in REG10 almeno annualmente e dopo qualsiasi modifica sostanziale all'ambito di applicazione del PIMS, al contesto legale, agli obblighi contrattuali o ai trattamenti ad alto rischio.

4.1.2 [All] L'Incident Response Coordinator DEVE registrare ogni incidente relativo ai dati personali sospetto segnalato o rilevato in REG10 entro un giorno lavorativo dalla ricezione, o prima quando può essere attivata una tempistica applicabile di notifica o di segnalazione al cliente.

4.1.3 [Both] Il System Owner / Application Owner DEVE conservare i log di sistema, gli allarmi, le registrazioni degli accessi, le evidenze di configurazione e le evidenze di ripristino pertinenti collegati a REG10 quando un incidente sospetto interessa un sistema o un'applicazione che tratta PII.

4.1.4 [Both] L'Information Security Lead DEVE completare il triage tecnico iniziale di qualsiasi evento di sicurezza che coinvolga PII entro 24 ore dalla rilevazione e registrare in REG10 la gravità iniziale, gli asset interessati e lo stato del contenimento.

4.2 Classificazione e valutazione della violazione

4.2.1 [Both] L'Incident Response Coordinator DEVE classificare ciascuna voce REG10 come evento non PII, incidente relativo ai dati personali sospetto, incidente relativo ai dati personali confermato o violazione dei dati personali confermata entro 24 ore dall'acquisizione, oppure aggiornare la registrazione REG10 con la motivazione per cui la classificazione resta in sospeso.

4.2.2 [Both] Il Privacy Lead / PIMS Manager DEVE identificare l'attività di trattamento, le categorie di PII, le categorie di interessati, i sistemi, i responsabili del trattamento, i sub-responsabili, le località di trasferimento e i rischi privacy interessati in REG02, REG04, REG08, REG09 e REG10 prima che la decisione di notifica della violazione sia finalizzata.

4.2.3 [Controller] Il Data Protection Officer / Privacy Advisor DEVE valutare il rischio per gli interessati coinvolti per ogni violazione dei dati personali confermata o ragionevolmente

sospetta e registrare in REG10 la raccomandazione di notifica, la motivazione del rischio e la consulenza prima che sia assunta la decisione di notifica esterna.

4.2.4 [Processor] Il Privacy Lead / PIMS Manager DEVE identificare il titolare del trattamento o cliente interessato e i requisiti contrattuali di notifica applicabili non appena l'organizzazione prende conoscenza di una violazione dei dati personali che interessa PII del cliente, e DEVE registrare l'esito in REG08 e REG10.

4.2.5 [Joint Controller] Il Privacy Lead / PIMS Manager DEVE verificare la responsabilità concordata per la violazione, la responsabilità primaria per le comunicazioni e l'assetto di coordinamento prima di qualsiasi notifica o comunicazione esterna da parte di un contitolare del trattamento, e DEVE registrare la decisione in REG08 e REG10.

4.2.6 [Conditional] Il Privacy Lead / PIMS Manager DEVE valutare i trigger applicabili di segnalazione legali, settoriali, del settore finanziario, di cibersicurezza, contrattuali, verso clienti e verso destinatari del servizio per ciascun incidente relativo ai dati personali ad alto impatto e registrare l'esito dell'applicabilità in REG01, REG08 e REG10.

[... Le sezioni 4.3–8 non sono incluse in questa anteprima. Acquistare il documento completo per accedere all'intero contenuto. ...]

9. Eccezioni

9.1.1 [Both] Il Privacy Lead / PIMS Manager DEVE registrare qualsiasi eccezione alla presente politica in REG12 prima dell'attuazione, oppure entro 24 ore dopo un'azione d'emergenza quando l'approvazione preventiva non era praticabile.

9.1.2 [Both] Top Management DEVE approvare qualsiasi eccezione che incida in modo rilevante sulle tempistiche di notifica della violazione, sulla comunicazione pubblica, sugli impegni verso i clienti, sulla conservazione delle evidenze o sul rischio per gli interessati prima della chiusura dell'incidente, con evidenza di approvazione conservata in REG10 e REG12.

9.1.3 [Conditional] Il Data Protection Officer / Privacy Advisor DEVE documentare la consulenza per qualsiasi notifica ritardata, decisione di mancata notifica o approccio di comunicazione eccezionale prima della chiusura dell'incidente, con consulenza conservata in REG10.

9.1.4 [Both] Il Vendor / Procurement Owner DEVE registrare in REG08 e REG12 le eccezioni determinate da fornitori, responsabili del trattamento, sub-responsabili o clienti che incidono sulla risposta agli incidenti entro cinque giorni lavorativi dall'identificazione dell'eccezione.

10. Applicazione della politica

10.1.1 [All] Il Process Owner / Business Owner DEVE sottoporre a escalation verso il Privacy Lead / PIMS Manager il mancato adempimento dell'obbligo di segnalare un incidente relativo ai dati personali sospetto, conservare evidenze, seguire le azioni assegnate o cooperare alla valutazione della violazione entro due giorni lavorativi dalla scoperta, con evidenze conservate in REG12.

10.1.2 [Both] Il Privacy Lead / PIMS Manager DEVE registrare una non conformità REG12 quando una violazione della presente politica incide su acquisizione dell'incidente, triage, contenimento, notifica, integrità delle evidenze, comunicazione o azione correttiva.

10.1.3 [Both] Il Vendor / Procurement Owner DEVE avviare la remediation del fornitore o del responsabile del trattamento tramite REG08 e REG12 entro cinque giorni lavorativi quando un responsabile del trattamento, sub-responsabile, fornitore o altra terza parte non rispetta gli obblighi concordati in materia di incidenti o violazioni.

10.1.4 [Both] Top Management DEVE riesaminare le non conformità rilevanti o ricorrenti nella gestione degli incidenti in occasione del successivo riesame della direzione programmato, con decisioni e azioni richieste conservate in REG12.

11. Riesame e manutenzione

11.1.1 [Both] Il Privacy Lead / PIMS Manager DEVE riesaminare la presente politica almeno annualmente e registrare in REG12 l'esito del riesame, le modifiche richieste e lo stato di approvazione.

11.1.2 [Both] L'Incident Response Coordinator DEVE attivare un riesame post-incidente della presente politica entro 30 giorni di calendario dalla chiusura di qualsiasi incidente relativo ai dati personali ad alto impatto o violazione dei dati personali confermata, con evidenze del riesame conservate in REG10 e REG12.

11.1.3 [Conditional] Il Privacy Lead / PIMS Manager DEVE riesaminare la presente politica entro 30 giorni di calendario dalla presa di conoscenza di una modifica rilevante ai requisiti applicabili di segnalazione degli incidenti legali, settoriali, verso clienti, contrattuali, relativi a responsabili del trattamento, sub-responsabili o trasferimenti, con evidenze del riesame conservate in REG01, REG08, REG09 e REG12.

11.1.4 [Both] L'Internal Audit / Compliance Reviewer DEVE riesaminare l'attuazione della presente politica almeno annualmente tramite il programma di audit interno PIMS, con risultanze dell'audit e azioni correttive conservate in REG12.

11.1.5 [Both] Top Management DEVE riesaminare tendenze degli incidenti, violazioni significative, prestazioni delle notifiche, azioni correttive scadute ed efficacia della politica durante il riesame della direzione programmato, con output conservati in REG12.

12. Politiche correlate

12.1 La presente politica deve essere letta insieme a:

12.2 PII01 - Politica del sistema di gestione delle informazioni sulla privacy

12.3 PII02 - Politica sui ruoli, le responsabilità e la responsabilizzazione privacy

12.4 PII03 - Politica sull'inventario dei trattamenti PII e sulla base giuridica

12.5 PII04 - Politica sull'informativa privacy e sulla trasparenza

12.6 PII06 - Politica di gestione dei diritti degli interessati

12.7 PII07 - Politica di valutazione del rischio privacy e DPIA

12.8 PII08 - Politica di privacy by design e privacy by default

12.9 PII10 - Politica di conservazione, cancellazione e smaltimento delle PII

12.10 PII12 - Politica di gestione privacy di responsabili del trattamento, sub-responsabili e terze parti

12.11 PII13 - Politica sui trasferimenti internazionali di PII

12.12 PII14 - Politica di sicurezza e controllo degli accessi alle PII

12.13 PII16 - Politica di formazione, sensibilizzazione e competenza privacy

12.14 PII17 - Politica di gestione delle informazioni documentate e delle evidenze PIMS

12.15 PII18 - Politica di monitoraggio, audit e miglioramento PIMS

13. Standard e quadri di riferimento

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].