					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : PII15					Titre du document : **Politique de gestion des incidents et des violations de données à caractère personnel**							
Version : 1.0		Date d'entrée en vigueur : 01.01.2025			Propriétaire du document :							
X	Politique		Norme		Procédure		Formulaire		Registre		Autre	

Historique des révisions				
Numéro de révision	**Date de révision**	**Modifications**	**Revu par**	**Propriétaire du processus**

Approbations			
Nom	**Fonction**	**Date**	**Signature**

Alignement sur les normes et réglementations

Norme / réglementation	Clause / mesure / article	Applicability	Coverage Type	Commentaire
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Communications du PIMS et éléments de preuve documentés relatifs aux violations
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Contrôle opérationnel, appréciation des risques relatifs à la vie privée et articulation avec le traitement des risques
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Surveillance, évaluation, non-conformité, action corrective et amélioration
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Planification et préparation de la gestion des incidents pour le traitement de données à caractère personnel
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Réponse aux incidents de sécurité de l'information impliquant des données à caractère personnel
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Exigences légales, statutaires, réglementaires et contractuelles, et protection des enregistrements
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Accord client du sous-traitant et appui aux obligations du client

GDPR	Article 5(2); Article 24	Controller	Supporting	Responsabilité et obligations du responsable du traitement
GDPR	Article 26	Joint Controller	Supporting	Coordination des responsabilités en matière de violation entre responsables conjoints du traitement
GDPR	Article 28	Both	Supporting	Assistance du sous-traitant et obligations contractuelles du sous-traitant
GDPR	Article 32	Both	Supporting	Sécurité du traitement et capacité de détection des violations
GDPR	Article 33	Both	Primary	Notification des violations de données à caractère personnel et documentation des violations
GDPR	Article 34	Controller	Primary	Communication des violations de données à caractère personnel aux personnes concernées affectées
GDPR	Article 39	Conditional	Supporting	Conseils du DPO, surveillance, coopération et appui comme point de contact
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Principes de sécurité de l'information et de conformité à la vie privée
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Responsabilités de réponse aux incidents relatifs aux données à

				caractère personnel et signalement des événements
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Planification, évaluation, réponse, retour d'expérience et collecte des éléments de preuve relatifs aux incidents
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Cycle de vie du processus de gestion des incidents
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Politique, plan, sensibilisation, tests et retours d'expérience relatifs aux incidents
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Opérations de détection, notification, triage, analyse, réponse et établissement de rapports
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Attentes relatives à la notification par le sous-traitant cloud et aux enregistrements de violation
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Signalement des incidents significatifs le cas échéant
DORA Regulation (EU) 2022/2554	Article 17; Article 18; Article 19	Conditional	Supporting	Gestion, classification et déclaration des incidents ICT le cas échéant

1. Champ d'application

1.1 La présente politique définit les exigences relatives à l'identification, au signalement, au triage, à l'évaluation, au confinement, à la notification, à la documentation, à la clôture et à l'amélioration à la suite d'incidents relatifs aux données à caractère personnel et de violations de données à caractère personnel dans le domaine d'application du PIMS.

1.2 La présente politique s'applique à :

1.2.1 l'organisation agissant en qualité de responsable du traitement de données à caractère personnel ;

1.2.2 l'organisation agissant en qualité de responsable conjoint du traitement lorsqu'une coordination des responsabilités en matière de violation est requise ;

1.2.3 l'organisation agissant en qualité de sous-traitant de données à caractère personnel ;

1.2.4 l'organisation agissant en qualité de sous-traitant ultérieur ;

1.2.5 les systèmes, applications, services, processus, fournisseurs, sous-traitants, sous-traitants ultérieurs et tiers qui traitent, stockent, transmettent, prennent en charge, consultent ou affectent autrement des données à caractère personnel dans le domaine d'application du PIMS.

1.3 La présente politique utilise REG10 - Registre des incidents et violations relatifs aux données à caractère personnel comme objet principal d'éléments de preuve pour la gestion des incidents et violations relatifs aux données à caractère personnel.

1.4 La présente politique utilise les objets d'éléments de preuve d'appui comme suit :

1.4.1 REG01 pour le domaine d'application du PIMS et le contexte applicable des parties intéressées, ainsi que le contexte légal, contractuel, sectoriel et client de reporting.

1.4.2 REG02 pour les activités de traitement affectées, les catégories de données à caractère personnel, les catégories de personnes concernées, les finalités et les systèmes.

1.4.3 REG03 pour la Déclaration d'applicabilité et les mises à jour de l'applicabilité des contrôles.

1.4.4 REG04 pour les liens avec le risque relatif à la vie privée, la DPIA et le risque résiduel.

1.4.5 REG08 pour les éléments de preuve relatifs aux interfaces d'incident avec les sous-traitants, sous-traitants ultérieurs, clients, fournisseurs et tiers.

1.4.6 REG09 pour les liens relatifs aux transferts internationaux lorsqu'un incident affecte un traitement transfrontière.

1.4.7 REG11 pour les éléments de preuve relatifs à la formation, à la sensibilisation et à la compétence en matière de réponse aux incidents.

1.4.8 REG12 pour les éléments de preuve relatifs à l'audit, aux non-conformités, aux actions correctives et à l'amélioration.

1.5 La présente politique s'appuie sur les politiques PIMS associées pour les contrôles spécialisés :

1.5.1 PII03 régit l'inventaire des traitements et les enregistrements de base légale.

1.5.2 PII04 régit les contrôles de mention d'information et de transparence en dehors des communications propres aux violations.

1.5.3 PII06 régit les demandes d'exercice des droits des personnes concernées qui surviennent avant, pendant ou après un incident.

1.5.4 PII07 régit la méthodologie d'appréciation des risques relatifs à la vie privée et de DPIA.

1.5.5 PII08 régit les contrôles de protection de la vie privée dès la conception et par défaut.

1.5.6 PII10 régit les contrôles de conservation, de suppression et d'élimination.

1.5.7 PII12 régit les contrôles relatifs aux relations avec les sous-traitants, sous-traitants ultérieurs, fournisseurs et tiers en matière de protection des données.

1.5.8 PII13 régit les outils de transfert international de données à caractère personnel et les enregistrements des risques de transfert.

1.5.9 PII14 régit les contrôles préventifs et détectifs de sécurité des données à caractère personnel et de contrôle d'accès.

1.5.10 PII16 régit la formation, la sensibilisation et la compétence en matière de vie privée.

1.5.11 PII17 régit les informations documentées et la gestion des éléments de preuve.

1.5.12 PII18 régit la surveillance, l'audit interne, la revue de direction, les non-conformités, les actions correctives et l'amélioration continue.

1.6 Aux fins de la présente politique :

1.6.1 « incident relatif aux données à caractère personnel » désigne un événement suspecté ou confirmé qui a affecté, pourrait avoir affecté ou pourrait raisonnablement affecter la confidentialité, l'intégrité, la disponibilité, le traitement licite ou le traitement autorisé de données à caractère personnel.

1.6.2 « violation de données à caractère personnel » désigne un incident confirmé relatif aux données à caractère personnel impliquant la destruction, la perte, l'altération, la divulgation, l'accès, l'indisponibilité ou la compromission non autorisés, illicites, accidentels ou non intentionnels de données à caractère personnel.

1.6.3 « évaluation d'une violation de données à caractère personnel » désigne l'évaluation documentée visant à déterminer si un incident relatif aux données à caractère personnel constitue une violation de données à caractère personnel, quelles données à caractère personnel et quelles personnes concernées sont affectées, quels risques peuvent survenir, quelles notifications ou communications sont requises et quelles actions de remédiation sont nécessaires.

1.6.4 « prise de connaissance » désigne le moment auquel l'organisation dispose d'un degré raisonnable de certitude qu'un incident de sécurité ou de vie privée est survenu et que des données à caractère personnel ont été ou peuvent avoir été compromises.

1.6.5 « incident à fort impact relatif aux données à caractère personnel » désigne un incident relatif aux données à caractère personnel impliquant un traitement à haut risque, des catégories particulières ou des données à caractère personnel hautement sensibles, des données à caractère personnel à grande échelle, des personnes vulnérables, des clients réglementés, un impact dans plusieurs juridictions, un impact matériel pour les clients, une compromission d'accès à privilèges, une exposition publique, un rançongiciel, une indisponibilité de service ou un impact opérationnel ou réputationnel significatif.

1.6.6 « modification substantielle relative à un incident » désigne toute information nouvelle ou modifiée affectant le périmètre de l'incident, sa gravité, les catégories de données à caractère personnel, l'impact sur les personnes concernées, la décision de notification, l'impact client, la cause racine, le confinement, le rétablissement, l'action corrective ou les obligations de reporting externe.

2. Objet

2.1 La présente politique a pour objet de garantir que les incidents et violations relatifs aux données à caractère personnel sont traités de manière cohérente, rapide, licite, sécurisée et compatible avec les exigences d'audit.

2.2 La présente politique soutient la responsabilité en exigeant que les incidents et violations relatifs aux données à caractère personnel soient enregistrés dans REG10 et reliés, lorsque cela est

déclenché, aux enregistrements de traitement affectés, aux risques relatifs à la vie privée, aux relations avec les sous-traitants et sous-traitants ultérieurs, aux enregistrements de transfert, aux actions correctives et aux enregistrements de formation.

2.3 La présente politique veille à ce que les obligations du responsable du traitement, du responsable conjoint du traitement, du sous-traitant et du sous-traitant ultérieur soient traitées au moyen de règles d'applicabilité distinctes, tout en maintenant un modèle intégré unique d'éléments de preuve relatifs aux incidents et violations.

3. Objectifs

3.1 Les objectifs de la présente politique sont les suivants :

3.1.1 garantir que les incidents suspectés relatifs aux données à caractère personnel sont signalés et enregistrés rapidement ;

3.1.2 garantir que les incidents relatifs aux données à caractère personnel sont soumis à triage et classifiés selon des critères cohérents ;

3.1.3 garantir que les évaluations d'une violation de données à caractère personnel prennent en compte les données à caractère personnel affectées, les personnes concernées, les systèmes, les activités de traitement, les sous-traitants, les sous-traitants ultérieurs, les transferts, les risques et les actions de remédiation ;

3.1.4 garantir que les décisions de notification par le responsable du traitement et de communication aux personnes concernées sont documentées ;

3.1.5 garantir que les notifications de violation par les sous-traitants et sous-traitants ultérieurs aux clients ou aux parties en amont sont effectuées sans retard indu et conformément aux accords applicables ;

3.1.6 garantir que les éléments de preuve sont préservés et protégés pendant la gestion de l'incident ;

3.1.7 garantir que le confinement, l'éradication, le rétablissement et la validation sont suivis au moyen de REG10 ;

3.1.8 garantir que les déclencheurs de reporting réglementaire, contractuel, client et sectoriel sont évalués le cas échéant ;

3.1.9 garantir que les retours d'expérience sur les incidents donnent lieu à des actions correctives et à une amélioration continue ;

3.1.10 garantir que les enregistrements d'incidents et de violations sont disponibles pour l'audit, la revue de direction, l'assurance client et la revue réglementaire le cas échéant.

4. Énoncés de politique

4.1 Préparation aux incidents et réception

4.1.1 [Both] Le Privacy Lead / PIMS Manager doit maintenir dans REG10 les critères de gestion des incidents et violations relatifs aux données à caractère personnel au moins une fois par an et après toute modification substantielle du domaine d'application du PIMS, du contexte légal, des obligations contractuelles ou des traitements à haut risque.

4.1.2 [All] L'Incident Response Coordinator doit enregistrer dans REG10 tout incident suspecté relatif aux données à caractère personnel signalé ou détecté dans un délai d'un jour ouvrable à compter de sa réception, ou plus tôt lorsqu'un délai applicable de notification ou de reporting client peut être déclenché.

4.1.3 [Both] Le System Owner / Application Owner doit préserver les journaux système, alertes, enregistrements d'accès, éléments de configuration et éléments de preuve de rétablissement pertinents liés à REG10 lorsqu'un incident suspecté affecte un système ou une application traitant des données à caractère personnel.

4.1.4 [Both] L'Information Security Lead doit achever le triage technique initial de tout événement de sécurité impliquant des données à caractère personnel dans les 24 heures suivant sa détection et enregistrer dans REG10 la gravité initiale, les actifs affectés et le statut du confinement.

4.2 Classification et évaluation d'une violation de données à caractère personnel

4.2.1 [Both] L'Incident Response Coordinator doit classifier chaque entrée REG10 comme événement ne concernant pas des données à caractère personnel, incident suspecté relatif aux données à caractère personnel, incident confirmé relatif aux données à caractère personnel ou violation confirmée de données à caractère personnel dans les 24 heures suivant la réception, ou mettre à jour l'enregistrement REG10 avec la raison pour laquelle la classification reste en attente.

4.2.2 [Both] Le Privacy Lead / PIMS Manager doit identifier l'activité de traitement affectée, les catégories de données à caractère personnel, les catégories de personnes concernées, les systèmes, les sous-traitants, les sous-traitants ultérieurs, les lieux de transfert et les risques relatifs à la vie privée dans REG02, REG04, REG08, REG09 et REG10 avant que la décision relative à la notification d'une violation de données à caractère personnel ne soit finalisée.

4.2.3 [Controller] Le Data Protection Officer / Privacy Advisor doit évaluer le risque pour les personnes concernées affectées pour chaque violation confirmée ou raisonnablement suspectée de données à caractère personnel et enregistrer dans REG10 la recommandation de notification, la justification du risque et ses conseils avant que la décision de notification externe ne soit prise.

4.2.4 [Processor] Le Privacy Lead / PIMS Manager doit identifier le responsable du traitement ou le client affecté ainsi que les exigences contractuelles de notification applicables dès que l'organisation prend connaissance d'une violation de données à caractère personnel affectant les données à caractère personnel du client, et doit consigner le résultat dans REG08 et REG10.

4.2.5 [Joint Controller] Le Privacy Lead / PIMS Manager doit vérifier la responsabilité convenue en matière de violation, la responsabilité principale de communication et le dispositif de coordination avant toute notification ou communication externe par un responsable conjoint du traitement, et doit consigner la décision dans REG08 et REG10.

4.2.6 [Conditional] Le Privacy Lead / PIMS Manager doit évaluer les déclencheurs applicables de reporting légal, sectoriel, financier, cybersécurité, contractuel, client et aux destinataires de service pour chaque incident à fort impact relatif aux données à caractère personnel, et consigner le résultat de l'applicabilité dans REG01, REG08 et REG10.

[... Les sections 4.3–8 ne sont pas incluses dans cet aperçu. Achetez le document complet pour accéder à l'intégralité du contenu. ...]

9. Exceptions

9.1.1 [Both] Le Privacy Lead / PIMS Manager doit enregistrer toute exception à la présente politique dans REG12 avant sa mise en œuvre, ou dans les 24 heures suivant une action d'urgence lorsqu'une approbation préalable n'était pas possible.

9.1.2 [Both] Top Management doit approuver toute exception affectant matériellement le calendrier de notification de violation, la communication publique, l'engagement client, la préservation des éléments de preuve ou le risque pour les personnes concernées avant la clôture de l'incident, les éléments de preuve d'approbation étant conservés dans REG10 et REG12.

9.1.3 [Conditional] Le Data Protection Officer / Privacy Advisor doit documenter ses conseils pour toute notification retardée, décision de non-notification ou approche exceptionnelle de communication avant la clôture de l'incident, les conseils étant conservés dans REG10.

9.1.4 [Both] Le Vendor / Procurement Owner doit enregistrer dans REG08 et REG12 les exceptions imposées par un fournisseur, sous-traitant, sous-traitant ultérieur ou client et affectant la réponse aux incidents dans les cinq jours ouvrables suivant l'identification de l'exception.

10. Application de la politique

10.1.1 [All] Le Process Owner / Business Owner doit escalader au Privacy Lead / PIMS Manager tout défaut de signalement d'un incident suspecté relatif aux données à caractère personnel, de préservation des éléments de preuve, de suivi des actions assignées ou de coopération à l'évaluation d'une violation de données à caractère personnel dans les deux jours ouvrables suivant sa découverte, les éléments de preuve étant conservés dans REG12.

10.1.2 [Both] Le Privacy Lead / PIMS Manager doit enregistrer une non-conformité REG12 lorsqu'un manquement à la présente politique affecte la réception des incidents, le triage, le confinement, la notification, l'intégrité des éléments de preuve, la communication ou l'action corrective.

10.1.3 [Both] Le Vendor / Procurement Owner doit initier la remédiation du fournisseur ou du sous-traitant au moyen de REG08 et REG12 dans les cinq jours ouvrables lorsqu'un sous-traitant, sous-traitant ultérieur, fournisseur ou autre tiers ne respecte pas les obligations convenues en matière d'incident ou de violation.

10.1.4 [Both] Top Management doit examiner les non-conformités matérielles ou récurrentes de gestion des incidents lors de la prochaine revue de direction planifiée, les décisions et actions requises étant conservées dans REG12.

11. Revue et maintenance

11.1.1 [Both] Le Privacy Lead / PIMS Manager doit examiner la présente politique au moins une fois par an et enregistrer le résultat de la revue, les modifications requises et le statut d'approbation dans REG12.

11.1.2 [Both] L'Incident Response Coordinator doit déclencher une revue post-incident de la présente politique dans les 30 jours calendaires suivant la clôture de tout incident à fort impact relatif aux données à caractère personnel ou de toute violation confirmée de données à caractère personnel, les éléments de preuve de revue étant conservés dans REG10 et REG12.

11.1.3 [Conditional] Le Privacy Lead / PIMS Manager doit examiner la présente politique dans les 30 jours calendaires après avoir pris connaissance d'une modification substantielle des exigences applicables de reporting d'incident légales, sectorielles, client, contractuelles, relatives aux sous-traitants, aux sous-traitants ultérieurs ou aux transferts, les éléments de preuve de revue étant conservés dans REG01, REG08, REG09 et REG12.

11.1.4 [Both] L'Internal Audit / Compliance Reviewer doit examiner la mise en œuvre de la présente politique au moins une fois par an dans le cadre du programme d'audit interne du PIMS, les constats d'audit et les actions correctives étant conservés dans REG12.

11.1.5 [Both] Top Management doit examiner les tendances des incidents, les violations significatives, la performance de notification, les actions correctives en retard et l'efficacité de la politique lors de la revue de direction planifiée, les résultats étant conservés dans REG12.

12. Politiques associées

12.1 La présente politique doit être lue conjointement avec :

12.2 PII01 - Politique du système de management des informations relatives à la vie privée

12.3 PII02 - Politique relative aux rôles, responsabilités et à la responsabilité en matière de vie privée

12.4 PII03 - Politique d'inventaire des traitements de données à caractère personnel et de base légale

12.5 PII04 - Politique relative aux mentions d'information et à la transparence

12.6 PII06 - Politique de gestion des droits des personnes concernées

12.7 PII07 - Politique d'appréciation des risques relatifs à la vie privée et de DPIA

12.8 PII08 - Politique de protection de la vie privée dès la conception et par défaut

12.9 PII10 - Politique de conservation, de suppression et d'élimination des données à caractère personnel

12.10 PII12 - Politique de gestion de la vie privée des sous-traitants, sous-traitants ultérieurs et tiers

12.11 PII13 - Politique de transfert international de données à caractère personnel

12.12 PII14 - Politique de sécurité des données à caractère personnel et de contrôle d'accès

12.13 PII16 - Politique de formation, de sensibilisation et de compétence en matière de vie privée

12.14 PII17 - Politique de gestion des informations documentées et des éléments de preuve du PIMS

12.15 PII18 - Politique de surveillance, d'audit et d'amélioration du PIMS

13. Normes et référentiels de référence

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].