					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : PII14					Titre du document : **Politique de sécurité et de contrôle d'accès de la PII**							
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**

Mentions légales (droits d'auteur et restrictions d'utilisation)

(C) 2025 Clarysec LLC. All rights reserved.

Le présent document est la propriété intellectuelle de Clarysec LLC. Aucune partie de ce document ne peut être copiée, réutilisée, distribuée ou modifiée à des fins commerciales ou de mise en œuvre sans autorisation écrite expresse préalable.

Toute utilisation non autorisée est strictement interdite et peut entraîner des poursuites judiciaires.

Pour toute demande de licence, contactez : info@clarysec.com

Alignement sur les normes et réglementations

Norme / Réglementation	Clause / Contrôle / Article	Applicabilité	Type de couverture	Commentaire
ISO/IEC 27701:2025	Clause 6.1.3; Clause 8.1	Both	Primary	Planification et exploitation des contrôles de sécurité de la PII
ISO/IEC 27701:2025	Clause 7.5; Clause 9.1; Clause 10.2	Both	Supporting	Éléments de preuve, surveillance et action corrective
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9	Both	Primary	Identité et droits d'accès pour le traitement de la PII
ISO/IEC 27701:2025	Annex A.3.22; Annex A.3.23	Both	Primary	Protection des terminaux et authentification sécurisée
ISO/IEC 27701:2025	Annex A.3.25; Annex A.3.26	Both	Primary	Journalisation et protection cryptographique
ISO/IEC 27701:2025	Annex A.3.28; Annex A.3.29	Both	Supporting	Sécurité des applications et architecture sécurisée
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.15; Annex A.3.16	Both	Supporting	Protection et revue des enregistrements
GDPR	Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32	Both	Primary	Sécurité, responsabilité et contrôles des sous-traitants
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Intégration des contrôles ISMS
ISO/IEC 27002:2022	Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Lignes directrices de mise en œuvre des contrôles de sécurité
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 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	Contrôles de sécurité pour la protection de la PII

1. Champ d’application

1.1 La présente politique définit les exigences propres à la PII en matière de sécurité et de contrôle d’accès pour les systèmes, applications, services, équipements, environnements cloud et processus opérationnels qui stockent, transmettent, traitent, consultent, administrent ou protègent la PII.

1.2 La présente politique s’applique aux contextes de responsable du traitement, de responsable conjoint du traitement, de sous-traitant et de sous-traitant ultérieur dans lesquels l’organisation détermine, exploite, soutient ou utilise des contrôles de sécurité pour le traitement de la PII.

1.3 La présente politique couvre les domaines de contrôle de sécurité de la PII suivants :

1.3.1 référentiel minimal de sécurité de la PII et intégration avec les politiques de sécurité de l’information existantes ;

1.3.2 contrôle d’accès ;

1.3.3 authentification ;

1.3.4 accès à privilèges ;

1.3.5 chiffrement et stockage sécurisé ;

1.3.6 journalisation et surveillance ;

1.3.7 configuration sécurisée et gestion des vulnérabilités ;

1.3.8 contrôles d’accès aux terminaux et au cloud ;

1.3.9 articulation des éléments de preuve au moyen de REG02, REG08, REG10 et REG12.

1.4 La présente politique ne remplace pas un système complet de management de la sécurité de l’information, une politique de sécurité réseau, une politique de développement sécurisé, une politique de sauvegarde, une politique relative aux terminaux, une politique de sécurité cloud, une norme de contrôle cryptographique, une procédure de gestion des vulnérabilités ou une procédure de réponse aux incidents. Lorsque ces politiques existent déjà, la présente politique définit les articulations propres à la PII et les exigences relatives aux éléments de preuve nécessaires à l’assurance du PIMS.

1.5 La présente politique ne duplique pas :

1.5.1 la responsabilité relative à l’inventaire des traitements de PII et à la base légale dans PII03 ;

1.5.2 la méthodologie d’appréciation des risques relatifs à la vie privée et de DPIA dans PII07 ;

1.5.3 les points de contrôle de protection de la vie privée dès la conception dans PII08 ;

1.5.4 les règles de collecte, d’utilisation, de divulgation et de partage dans PII09 ;

1.5.5 l’exécution de la conservation, de la suppression et de l’élimination dans PII10 ;

1.5.6 la gouvernance du cycle de vie des sous-traitants dans PII12 ;

1.5.7 les contrôles des outils de transfert international dans PII13 ;

1.5.8 le processus relatif aux incidents et aux violations dans PII15 ;

1.5.9 la gouvernance des informations documentées dans PII17 ;

1.5.10 la gouvernance de la surveillance, de l’audit et de l’amélioration du PIMS dans PII18.

1.6 Pour la présente politique, les journaux opérationnels, les sorties des outils de sécurité, les exports de revue d’accès, les rapports de vulnérabilités et les éléments de preuve de configuration constituent des sources d’éléments de preuve jointes aux objets de preuve canoniques, résumées dans ceux-ci ou référencées par ceux-ci. Ils ne constituent pas des registres PIMS distincts.

2. Objet

2.1 La présente politique a pour objet de veiller à ce que la PII soit protégée par des contrôles de sécurité et de contrôle d'accès appropriés, alignés sur les risques et auditables tout au long du traitement.

2.2 La présente politique permet à l'organisation de démontrer que les contrôles de sécurité de la PII sont planifiés, mis en œuvre, revus, surveillés et améliorés au moyen de REG02, REG08, REG10 et REG12, sans créer de registres de sécurité en double ni remplacer les politiques de sécurité de l'information existantes.

3. Objectifs

3.1 Les objectifs de la présente politique sont les suivants :

3.1.1 définir un référentiel minimal de contrôle d'accès à la PII pour les systèmes et les activités de traitement ;

3.1.2 veiller à ce que les contrôles d'authentification soient appropriés à la sensibilité de la PII et au contexte d'accès ;

3.1.3 définir les exigences de revue des accès à privilèges et des accès ordinaires à la PII ;

3.1.4 définir les attentes en matière de chiffrement et de stockage sécurisé de la PII au repos, en transit et dans les contextes cloud ou de terminaux pertinents ;

3.1.5 définir les attentes en matière de journalisation et de surveillance pour l'accès à la PII, les modifications de la PII et l'administration de la PII ;

3.1.6 définir les exigences relatives aux éléments de preuve de configuration sécurisée et de vulnérabilités pour les systèmes traitant la PII ;

3.1.7 définir les attentes relatives aux accès depuis les terminaux et le cloud sans créer une politique complète de sécurité des terminaux ou du cloud ;

3.1.8 relier les incidents de sécurité suspectés concernant la PII à REG10 sans dupliquer le processus de gestion des incidents ;

3.1.9 s'intégrer aux politiques de sécurité de l'information existantes lorsqu'elles sont disponibles ;

3.1.10 maintenir des éléments de preuve compatibles avec les exigences d'audit en utilisant uniquement REG02, REG08, REG10 et REG12.

4. Énoncés de politique

4.1 Référentiel minimal de sécurité de la PII et intégration ISMS

4.1.1 [Both] The Information Security Lead MUST définir le référentiel minimal de sécurité de la PII pour chaque système ou service qui traite la PII dans REG12 avant que le système ou service n'entre en production ou ne fasse l'objet d'une modification substantielle.

4.1.2 [Both] The System Owner / Application Owner MUST consigner l'emplacement des éléments de preuve relatifs aux contrôles de sécurité de la PII mis en œuvre dans REG12 avant de s'appuyer sur un contrôle de sécurité de l'information existant pour l'assurance du PIMS.

4.1.3 [Controller] The Process Owner / Business Owner MUST identifier la sensibilité de la PII, le contexte de traitement et le besoin d'accès dans REG02 avant de demander un accès nouveau ou substantiellement modifié à la PII.

4.1.4 [Processor] The Vendor / Procurement Owner MUST consigner les instructions de sécurité du client, les périmètres des responsabilités du client et les engagements de sécurité du sous-traitant dans REG08 avant le début ou la modification substantielle de l'accès du sous-traitant à la PII du client.

4.1.5 [Both] The Privacy Lead / PIMS Manager MUST vérifier que les éléments de preuve relatifs à la sécurité de la PII sont reliés à REG02, REG08, REG10 ou REG12 avant d'accepter l'activité de traitement comme auditable au titre du PIMS.

4.2 Référentiel minimal de contrôle d'accès

4.2.1 [Both] The System Owner / Application Owner MUST restreindre l'accès à la PII aux rôles approuvés et aux utilisateurs autorisés consignés ou traçables dans REG02 ou REG12 avant l'activation de l'accès.

4.2.2 [Both] The Process Owner / Business Owner MUST approuver la finalité métier de l'accès à la PII dans REG02 ou REG12 avant que The System Owner / Application Owner n'attribue l'accès.

4.2.3 [Both] The System Owner / Application Owner MUST revoir les accès utilisateurs aux systèmes traitant de la PII à fort impact ou sensible au moins une fois par trimestre et consigner le résultat de la revue dans REG12.

4.2.4 [Both] The System Owner / Application Owner MUST revoir les accès utilisateurs aux autres systèmes traitant la PII au moins une fois par an et consigner le résultat de la revue dans REG12.

4.2.5 [Both] The System Owner / Application Owner MUST supprimer ou modifier l'accès à la PII dans REG12 dans un délai d'un jour ouvré après un changement de rôle, un départ, la finalisation du contrat ou lorsque l'accès n'est plus requis.

4.2.6 [Processor] The Vendor / Procurement Owner MUST confirmer dans REG08 que l'accès du sous-traitant à la PII du client est limité aux instructions documentées du client avant l'activation ou la modification de l'accès.

4.2.7 [Subprocessor] The Vendor / Procurement Owner MUST confirmer dans REG08 que l'accès du sous-traitant ultérieur à la PII est limité aux activités de sous-traitance autorisées avant l'activation ou la modification de l'accès du sous-traitant ultérieur.

[... 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] The Information Security Lead MUST consigner chaque exception à une exigence de sécurité ou de contrôle d'accès de la PII dans REG12 avant l'activation de l'exception.

9.1.2 [Both] The Data Protection Officer / Privacy Advisor MUST conseiller sur les exceptions de sécurité de la PII à risque plus élevé dans REG12 avant approbation.

9.1.3 [Both] Top Management MUST approuver les exceptions de sécurité de la PII dans REG12 avant activation lorsque l'exception affecte de la PII à fort impact, de la PII sensible, l'accès à privilèges, le chiffrement, la journalisation ou des vulnérabilités à haut risque non résolues.

9.1.4 [Both] The Information Security Lead MUST définir la date d'expiration de l'exception, le contrôle compensatoire et la date de revue dans REG12 avant l'approbation de l'exception.

9.1.5 [Both] The System Owner / Application Owner MUST remédier aux exceptions de sécurité de la PII expirées, les renouveler ou les clôturer dans REG12 dans un délai de cinq jours ouvrés après expiration.

9.1.6 [Processor] The Vendor / Procurement Owner MUST consigner les exceptions de sécurité du sous-traitant ou du sous-traitant ultérieur affectant la PII du client dans REG08 et REG12 avant acceptation.

10. Application de la politique

10.1.1 [Both] The Privacy Lead / PIMS Manager MUST consigner les non-conformités relatives aux éléments de preuve de sécurité de la PII manquants ou incomplets dans REG12 dans un délai de cinq jours ouvrés après identification.

10.1.2 [Both] The Information Security Lead MUST attribuer la responsabilité de la remédiation des défaillances de contrôles de sécurité de la PII dans REG12 dans un délai de cinq jours ouvrés après validation.

10.1.3 [Both] The System Owner / Application Owner MUST désactiver ou restreindre les accès à la PII non autorisés, excessifs ou non étayés dans un délai d'un jour ouvré après validation et consigner l'action dans REG12.

10.1.4 [Conditional] The Incident Response Coordinator MUST relier les mesures d'application à REG10 dans un délai d'un jour ouvré lorsque la mesure d'application concerne un incident suspecté ou confirmé relatif à la PII.

10.1.5 [Both] Top Management MUST revoir les non-conformités de sécurité de la PII répétées ou à haut risque dans REG12 avant la revue de direction.

11. Revue et maintenance

11.1.1 [All] The Privacy Lead / PIMS Manager MUST revoir la présente politique avec The Information Security Lead au moins une fois par an et consigner le résultat de la revue dans REG12.

11.1.2 [Both] The Information Security Lead MUST revoir le référentiel minimal de sécurité de la PII dans REG12 dans un délai de 30 jours après tout changement substantiel de technologie, de menace, d'audit, d'incident ou de réglementation affectant la sécurité de la PII.

11.1.3 [Both] The System Owner / Application Owner MUST mettre à jour les éléments de preuve de sécurité de la PII au niveau du système dans REG12 dans un délai de 30 jours après tout changement substantiel d'architecture, d'accès, de configuration, de vulnérabilité ou de journalisation.

11.1.4 [Processor] The Vendor / Procurement Owner MUST revoir les éléments de preuve relatifs aux responsabilités de sécurité de la PII des sous-traitants et sous-traitants ultérieurs dans REG08 dans un délai de 30 jours après toute modification substantielle de service, d'instruction du client ou de sous-traitant ultérieur.

11.1.5 [All] The Internal Audit / Compliance Reviewer MUST vérifier les éléments de preuve de revue de la politique et certains éléments de preuve de contrôles de sécurité de la PII dans REG12 conformément au plan d'audit approuvé.

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 relative à l'inventaire des traitements de PII et à la base légale ;

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

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

12.7 PII09 - Politique de collecte, d'utilisation, de divulgation et de partage de la PII ;

12.8 PII10 - Politique de conservation, de suppression et d'élimination de la PII ;

12.9 PII12 - Politique de gestion de la protection des données des sous-traitants, sous-traitants ultérieurs et tiers ;

12.10 PII13 - Politique relative aux transferts internationaux de PII ;

12.11 PII15 - Politique de gestion des incidents et violations concernant la PII ;

12.12 PII16 - Politique relative à la formation, à la sensibilisation et à la compétence en matière de vie privée ;

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

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

13. Normes et référentiels de référence

13.1 ISO/IEC 27701:2025 - Clause 6.1.3; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.7; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5; 5.1.4; 5.1.6; 6.1.2; 7.1.1; 7.1.2].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.5.5; 4.6.3; 4.6.4; 4.7.5; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 7.1.3; 7.1.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.2; 11.1.1; 11.1.5].

13.3 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 10.1.3].

13.4 ISO/IEC 27701:2025 - Annex A.3.22; Annex A.3.23. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5].

13.5 ISO/IEC 27701:2025 - Annex A.3.25; Annex A.3.26. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.6 ISO/IEC 27701:2025 - Annex A.3.28; Annex A.3.29. Addressed by clauses [4.1.1; 4.1.2; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 7.1.1; 7.1.2].

13.7 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.15; Annex A.3.16. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.6.2; 4.6.3; 4.6.4; 4.7.2; 4.7.3; 5.1.9; 6.1.6; 8.1.4; 10.1.1; 11.1.5].

13.8 GDPR - Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.5; 4.2.6; 4.2.7; 4.3.2; 4.4.4; 4.5.1; 4.5.2; 4.6.1; 4.6.6; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 4.8.5; 5.1.1; 5.1.7; 6.1.4; 7.1.4; 9.1.3; 10.1.4].

13.9 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.10 ISO/IEC 27002:2022 - Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.11 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.1; 4.5.1; 4.6.2; 4.6.6; 4.7.6; 5.1.2; 6.1.1; 8.1.4; 10.1.1; 11.1.1].

13.12 ISO/IEC 29151:2022 - Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.7.1; 4.7.2; 4.7.4; 4.8.1; 4.8.2; 6.1.6; 11.1.5].