					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P07					Titre du document : **Politique d'intégration et de départ**							
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/Article	Commentaire
ISO/IEC 27001:2022	Clause 7.2, Clause 6	Compétence du personnel, intégration sécurisée et application des responsabilités lors du départ ou du changement de poste.
ISO/IEC 27002:2022	Contrôles 6.2, 6.5, 5	Contrôles relatifs à l'intégration, aux accès et au cycle de vie du personnel.
NIST SP 800-53 Rév. 5	PS-4, PS-5, AC-2, AC-6, IA-4, IA-5, CM-5, AU-2, AU-6	Transition et départ du personnel, moindre privilège, journalisation d'audit et gestion des accès pendant et après les changements de situation du personnel.
RGPD de l'UE	Articles 5(1)(f), 25, 32 ; considérant 39	Limitation des accès, confidentialité, protection et contrôles appropriés relatifs aux données du personnel.
NIS2 de l'UE	Article 21(2)(b, c, d)	Mesures de sécurité du personnel et de sécurité opérationnelle ; atténuation de la menace interne ; processus de cycle de vie.
DORA de l'UE	Articles 5, 8, 9	Gouvernance, contrôle interne des TIC, risque lié aux TIC et gestion des incidents lors des transitions du personnel.
COBIT 2019	APO07, BAI08, DSS05, MEA03	Ressources humaines, gestion des connaissances, sécurité et conformité dans les processus d'intégration et de départ.

1. Objet

1.1 La présente politique établit des procédures normalisées pour gérer l'intégration, les mobilités internes et les départs pour tous les types d'utilisateurs.

1.2 Elle garantit l'attribution et la suppression des accès physiques et logiques en temps utile et de manière sécurisée, tout en imposant la confidentialité, la responsabilité et la restitution des actifs.

1.3 La présente politique atténue les risques liés aux accès non autorisés, à la fuite de données et aux actifs non restitués en intégrant les contrôles d'intégration et de départ dans les processus des ressources humaines, les processus informatiques et les processus de sécurité.

1.4 Elle contribue à la mesure 6 de l'Annexe A de l'ISO/IEC 27001:2022 en garantissant l'application des obligations de sécurité du personnel pendant et après l'emploi ou l'engagement.

2. Champ d'application

2.1 La présente politique s'applique à tous les employés, prestataires, consultants, fournisseurs et autres tiers disposant d'un accès aux systèmes, réseaux, installations ou données de l'organisation.

2.2 Elle régit l'ensemble du cycle de vie suivant :

2.2.1 intégration (embauche, contractualisation ou engagement temporaire)

2.2.2 mobilité interne ou changement de rôle

2.2.3 départ (démission, retraite, licenciement, expiration du contrat)

2.3 La politique couvre :

2.3.1 l'accès logique (systèmes, applications, cloud, VPN)

2.3.2 l'accès physique (badges, clés, systèmes de contrôle d'accès aux bâtiments)

2.3.3 les actifs attribués (ordinateurs portables, téléphones, jetons, identifiants)

2.3.4 l'attestation de prise de connaissance des politiques et des obligations de confidentialité

2.4 Tous les départements (ressources humaines, informatique, services généraux, sécurité et management) sont responsables de l'exécution de leur rôle dans les flux de travail d'intégration et de départ.

3. Objectifs

3.1 Garantir que l'accès n'est accordé à un membre du personnel qu'après satisfaction des prérequis de sécurité, de formation et contractuels.

3.2 Révoquer les droits d'accès et récupérer les actifs de l'organisation immédiatement lors d'un changement de rôle ou d'un départ.

3.3 Préserver la confidentialité, l'intégrité et la disponibilité des actifs de l'organisation lors des transitions du personnel.

3.4 Garantir la traçabilité à des fins d'audit et la défendabilité juridique au moyen d'enregistrements complets des événements d'intégration et de départ.

3.5 Réduire l'exposition à la menace interne en validant et en documentant tous les événements d'accès liés au personnel.

3.6 Aligner le cycle de vie du personnel de l'organisation sur des pratiques de sécurité fondées sur les risques et sur les exigences réglementaires.

4. Rôles et responsabilités

4.1 Haute direction

4.1.1 Approuve la présente politique et alloue l'autorité ainsi que les ressources nécessaires aux processus d'intégration, de départ et de contrôle d'accès.

4.1.2 Veille à ce que les transitions du personnel n'exposent pas l'organisation à un risque de sécurité ou à un risque juridique indu.

4.2 Ressources humaines (RH)

4.2.1 Déclenchent les flux de travail d'intégration et de départ pour les employés et notifient les départements concernés des changements.

4.2.2 Veillent à ce que les vérifications d'antécédents, les contrats, les accords de non-divulgation et les attestations de prise de connaissance de la politique soient finalisés avant l'octroi des accès.

4.2.3 Informent l'informatique et les services généraux des départs du personnel conformément au délai de notification défini.

4.2.4 Se coordonnent avec les affaires juridiques pour faire appliquer les obligations post-contractuelles ou postérieures à l'emploi (par exemple, les clauses de non-divulgation).

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

9. Exigences de revue et de mise à jour

9.1 Fréquence de revue de la politique

9.1.1 La présente politique doit faire l'objet d'une revue :

9.1.1.1 annuellement, ou

9.1.1.2 après tout incident significatif impliquant un usage abusif des accès, une perte d'actifs ou une défaillance procédurale

9.1.1.3 lors de la mise en œuvre de changements majeurs des RH ou de la plateforme IAM

9.1.1.4 à la suite de mises à jour réglementaires ou juridiques affectant les données du personnel ou les obligations applicables

9.2 Processus de revue et responsabilité

9.2.1 Le responsable du SMSI et le directeur des ressources humaines doivent coordonner la revue, avec la contribution de la sécurité informatique, des affaires juridiques et de la conformité.

9.2.2 Toute modification doit être approuvée par la haute direction et le comité de pilotage du SMSI.

9.2.3 Les versions révisées doivent être redistribuées aux départements et membres du personnel concernés pour nouvelle attestation de prise de connaissance.

9.3 Contrôle documentaire et conservation

9.3.1 La présente politique doit inclure :

9.3.2 la gestion des versions, l'historique des changements et la date d'entrée en vigueur

9.3.3 le propriétaire du document et le ou les réviseurs

9.3.4 la classification de la politique et la preuve d'approbation

9.3.5 Les versions obsolètes doivent être archivées pendant au moins 3 ans conformément à la politique de gestion documentaire.

10. Politiques associées et articulations

10.1.1 La présente politique s'articule directement avec :

10.1.2 P1 – Politique de sécurité de l'information : établit les objectifs de sécurité de l'organisation, y compris la gouvernance des accès du personnel.

10.1.3 P4 – Politique de contrôle d'accès : définit les exigences opérationnelles d'attribution et de révocation des accès aux systèmes et des accès physiques sur la base des déclencheurs d'intégration et de départ.

10.1.4 P3 – Politique d'utilisation acceptable : impose une attestation de prise de connaissance lors de l'intégration et soutient son application après le départ.

10.1.5 P6 – Politique de gestion des risques : garantit que les risques liés aux accès utilisateurs et aux transitions sont évalués et traités conformément aux principes du SMSI.

10.1.6 P11 – Politique de gestion des comptes utilisateurs et des privilèges : régit les contrôles techniques d'attribution et de suppression des accès à l'appui de la présente politique.

10.2 Ces politiques forment un dispositif de contrôle intégré permettant de gérer de manière sécurisée et responsable les événements du cycle de vie du personnel.

11. Normes et référentiels de référence

11.1 La présente politique est alignée sur des référentiels reconnus en matière de sécurité, de protection de la vie privée et de gouvernance des TI afin de garantir que les processus d'intégration et de départ sont sécurisés, traçables et conformes aux exigences juridiques et organisationnelles.

11.2 ISO/IEC 27001:

11.2.1 Clause 7.2 – Compétence et Clause 6.2 – Objectifs de sécurité de l'information : la présente politique soutient l'établissement de la compétence du personnel et l'intégration sécurisée des personnes dans des rôles influençant les objectifs du SMSI.

11.2.2 Annexe A, mesure 6.5 – Responsabilités après le départ ou le changement d'emploi : la présente politique impose pleinement les contrôles relatifs aux droits d'accès résiduels, à la détention des données et aux obligations contractuelles lors du départ.

11.2.3 Annexe A, mesure 5.9 – Vérification préalable et 6.2 – Conditions d'emploi : les procédures d'intégration intègrent des mécanismes de vérification des antécédents et d'attestation de prise de connaissance de la politique conformes à ces clauses.

11.3 NIST SP 800-53 Rév. 5:

11.3.1 PS-4 (Personnel Termination) et PS-5 (Personnel Transfer) : la présente politique impose la suppression ou la modification structurée des droits d'accès, des badges physiques et des actifs.

11.3.2 AC-2 (Account Management) et AC-6 (Least Privilege) : les dispositions garantissent que les accès sont alignés sur le rôle et révoqués sans délai lorsqu'ils ne sont plus nécessaires.

11.3.3 IA-4 (Identifier Management) et IA-5 (Authenticator Management) : la politique soutient la gestion sécurisée des identifiants pendant et après les changements concernant le personnel.

11.3.4 CM-5 (Access Restrictions for Change) : la politique empêche les changements non autorisés après départ par la révocation des droits d'accès élevés.

11.3.5 AU-2 et AU-6 : la journalisation et la traçabilité des événements d'accès sont renforcées grâce à l'intégration avec l'IAM et à la piste d'audit.

11.4 RGPD de l'UE (2016/679):

11.4.1 Article 5(1)(f) : protège les données à caractère personnel contre les accès non autorisés, notamment par la révocation des accès utilisateurs lors du départ.

11.4.2 Article 32 : impose des contrôles techniques et organisationnels appropriés pour sécuriser les données à caractère personnel tout au long du cycle d'emploi.

11.4.3 Article 25 – protection des données dès la conception : garantit que l'intégration et le départ intègrent la minimisation des données, la conservation et les contrôles d'accès licites.

11.4.4 Considérant 39 : souligne la limitation des accès et la confidentialité, soutenues par la structure de la présente politique.

11.5 Directive NIS2 de l'UE (2022/2555):

11.5.1 Article 21(2)(b, c, d) : exige des mesures de sécurité du personnel et de sécurité opérationnelle couvrant le contrôle d'accès, l'atténuation de la menace interne et les processus du cycle de vie, tous reflétés dans la présente politique.

11.6 DORA de l'UE (2022/2554):

11.6.1 Article 5 – Gouvernance et contrôle interne : la présente politique soutient la gouvernance interne des TIC en lien avec le risque humain et la gestion des accès.

11.6.2 Article 8 – Gestion des risques liés aux TIC : applique des contrôles aux transitions du personnel susceptibles d'exposer des actifs critiques ou des environnements réglementés.

11.6.3 Article 9 – Classification et gestion des incidents : garantit que les violations liées au départ sont notifiées et atténuées au moyen d'une suppression appropriée des accès et d'une gestion adéquate des actifs.

11.7 COBIT 2019:

11.7.1 APO07 – Managed Human Resources : définit les rôles, responsabilités et actions du cycle de vie pour l'intégration et le départ en cohérence avec les objectifs de gouvernance.

11.7.2 BAI08 – Knowledge Management : renforce la documentation des procédures, la conservation des connaissances et le transfert de contrôle à la fin de l'emploi.

11.7.3 DSS05 – Managed Security Services : impose la désactivation des utilisateurs, le contrôle des actifs et la responsabilité lors des transitions de rôle.

11.7.4 MEA03 – Monitor, Evaluate, and Assess Compliance : garantit que les contrôles d’intégration et de départ sont évalués lors des audits internes et externes.