					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P07S					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	Clauses 6.2, 7	Exigences relatives à la sécurité des ressources humaines et à la sensibilisation
ISO/IEC 27002:2022	Mesures 6.2, 6.5	Pratiques de sécurité relatives à l'intégration et au départ
NIST SP 800-53 Rev.5	PS-4, AC-2, PL-4	Départ du personnel ; cycle de vie des comptes ; planification
Directive NIS2 de l'UE	Article 21(2)(h)	Sécurité des ressources humaines et cycle de vie des accès
Règlement DORA de l'UE	Article 12	Contrôles d'accès et révocation pour les systèmes TIC
COBIT 2019	APO07, DSS01	Sécurité du personnel, contrôles d'accès logique et physique
RGPD de l'UE	Article 32	Sécurité des données à caractère personnel pendant la relation de travail

1. Objet

1.1 La présente politique définit le processus d'intégration des nouveaux employés et prestataires ainsi que la suppression sécurisée des accès lorsque des personnes quittent l'organisation ou changent de fonction.

1.2 Elle exige que les accès soient attribués selon le principe du moindre privilège, que tous les actifs fassent l'objet d'un suivi et que les actions critiques, telles que la désactivation des systèmes et la récupération des données, soient réalisées dans les délais requis.

1.3 La présente politique contribue à la conformité, à l'intégrité opérationnelle et à la protection des données au moyen d'activités d'intégration et de départ structurées et traçables à des fins d'audit.

2. Champ d'application

2.1 La présente politique s'applique à :

2.1.1 tous les employés permanents et temporaires ;

2.1.2 les prestataires, consultants et stagiaires ;

2.1.3 les prestataires de services externes disposant d'un accès aux systèmes ou d'un accès physique.

2.2 Elle couvre :

2.2.1 l'intégration : création de comptes utilisateurs, octroi des accès, attribution des équipements ;

2.2.2 le départ : suppression des accès, récupération des actifs de l'entreprise et clôture sécurisée des identités numériques ;

2.2.3 les changements de fonction internes nécessitant une reconfiguration des accès ou une réattribution des actifs.

2.3 Elle s'applique à tous les équipements, plateformes et sites utilisés dans le cadre des activités professionnelles officielles.

3. Objectifs

3.1 Veiller à ce que les nouveaux membres du personnel reçoivent les accès et ressources correspondant à des rôles et responsabilités vérifiés.

3.2 Veiller à ce que les utilisateurs sortants soient intégralement retirés des systèmes et des locaux au plus tard à la fin de leur dernier jour ouvré.

3.3 Prévenir l'existence de comptes orphelins et d'actifs non restitués, qui constituent un risque de sécurité.

3.4 Tenir des enregistrements documentés des actions d'intégration, de mobilité interne et de départ.

3.5 Renforcer la responsabilisation au moyen de listes de contrôle et d'une coordination interfonctionnelle des rôles.

4. Rôles et responsabilités

4.1 Directeur général

4.1.1 Approuve les accès associés aux rôles à privilèges élevés et supervise le programme d'intégration et de départ.

4.1.2 Veille à ce que les dérogations soient justifiées et à ce que des actions correctives soient engagées lorsque les processus ne sont pas respectés.

4.2 Responsable administratif / Ressources humaines

4.2.1 Déclenche le processus d'intégration des nouveaux arrivants et informe l'informatique des départs.

4.2.2 Veille à l'établissement des documents juridiques requis (par exemple, accord de non-divulgation) et des attestations de prise de connaissance des politiques de sécurité.

4.2.3 Tient à jour les listes de contrôle d'intégration et de départ et contrôle la conformité à la présente politique.

[... 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 Revue annuelle

9.1.1 La présente politique doit faire l'objet d'une revue au moins une fois par an par le directeur général et les responsables des ressources humaines et de l'informatique.

9.2 Déclencheurs de revue anticipée

9.2.1 Une mise à jour doit intervenir si :

9.2.1.1 de nouveaux systèmes RH ou informatiques sont introduits ;

9.2.1.2 il y a un changement de prestataire de services informatiques externe ou de service RH externalisé ;

9.2.1.3 des audits de sécurité révèlent des lacunes de processus ;

9.2.1.4 les obligations réglementaires évoluent (par exemple, mises à jour du RGPD) ;

9.2.1.5 une défaillance critique du processus de départ ou une violation survient.

9.3 Gestion des versions et approbation

9.3.1 Chaque version de la présente politique doit inclure :

9.3.1.1 un numéro de version et une date ;

9.3.1.2 un résumé des modifications ;

9.3.1.3 l'approbation du directeur général ;

9.3.1.4 les versions antérieures archivées, conservées pendant au moins trois ans.

9.4 Communication et prise de connaissance

9.4.1 Tout le personnel chargé de l'intégration ou du départ doit être informé de toute mise à jour de la politique. Des sessions annuelles de sensibilisation ou de rappel sont obligatoires.

10. Politiques connexes et articulations

10.1 La présente politique s'articule avec les documents suivants et les soutient :

10.1.1 P2S – Politique relative aux rôles et responsabilités de gouvernance : encadre la responsabilisation dans les processus d'accès et d'intégration.

10.1.2 P4S – Politique de contrôle d'accès : établit la mise en œuvre technique de l'attribution fondée sur les rôles et de la désactivation.

10.1.3 P6S – Politique de gestion des risques : évalue les risques résultant des défaillances de contrôle liées à l'intégration et au départ.

10.1.4 P8S – Politique de sensibilisation et de formation à la sécurité de l'information : impose les exigences d'accueil du personnel lors de l'intégration.

10.1.5 P30S – Politique de réponse aux incidents : traite comme des incidents de sécurité l'absence de suppression des accès ou le vol d'actifs.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001

11.1.1 Clause 6.2 – Établit les exigences de sécurité des ressources humaines.

11.1.2 Clause 7.2 – Rend obligatoire la formation de sensibilisation pour les nouveaux membres du personnel.

11.2 ISO/IEC 27002

11.2.1 Mesures 6.2 et 6.5 – Détaille les pratiques de sécurité relatives à l'intégration et au départ des employés.

11.3 NIST SP 800-53 Rev. 5

11.3.1 PS-4 – Procédures de départ du personnel, y compris la désactivation des accès.

11.3.2 AC-2 – Exige la gestion du cycle de vie des comptes pour les accès utilisateurs.

11.3.3 PL-4 – Exige la planification des transitions du personnel.

11.4 RGPD de l'UE

11.4.1 Article 32 – Exige un niveau de sécurité approprié pendant et après la relation de travail, en particulier pour l'accès aux données à caractère personnel.

11.5 Directive NIS2 de l'UE

11.5.1 Article 21(2)(h) – Exige des contrôles relatifs à la sécurité des ressources humaines et au cycle de vie des accès.

11.6 Règlement DORA de l'UE

11.6.1 Article 12 – Exige des entités financières réglementées qu'elles maîtrisent les accès du personnel aux systèmes TIC, y compris les procédures de révocation.

11.7 COBIT 2019

11.7.1 APO07 – Gérer les ressources humaines : établit les exigences de sécurité relatives au cycle de vie du personnel.

11.7.2 DSS01 – Gérer les opérations : couvre le contrôle des accès logiques et physiques lors des transitions d'emploi.