					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P11S					Titre du document : **Politique de gestion des comptes utilisateurs et des privilèges**							
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 5.3, 8	Rôles, responsabilités, planification et maîtrise opérationnelle applicables à la gestion des accès utilisateurs
ISO/IEC 27002:2022	Mesure 8	Contrôles relatifs à l'attribution, à la revue et à la suppression des privilèges élevés
NIST SP 800-53 Rev.5	AC-2, AC-5, AC-6	Création des comptes, surveillance, moindre privilège et séparation des tâches
Directive NIS2 de l'UE	Article 21(2)(d)	Gestion des accès utilisateurs pour les entités essentielles et importantes
Règlement DORA de l'UE	Article 9(2)(b)	Contrôle des accès à privilèges au sein des entités financières
COBIT 2019	DSS05.03, DSS05.04	Attribution, suppression et revue périodique des accès utilisateurs
RGPD	Article 32	Contrôles d'accès appropriés pour la protection des données à caractère personnel

1. Objet

1.1 La présente politique définit les règles de gestion des comptes utilisateurs et des droits d'accès de manière sécurisée, cohérente et traçable. Elle garantit que seuls les utilisateurs autorisés accèdent aux systèmes et aux données, et que cet accès est adapté à leur rôle et à leurs responsabilités.

1.2 Une gestion efficace des comptes et des privilèges est essentielle pour prévenir les accès non autorisés, réduire les risques de menace interne et garantir la conformité à l'ISO/IEC 27001, au RGPD et aux autres exigences réglementaires applicables.

1.3 La présente politique permet à l'organisation d'attribuer clairement la propriété et la responsabilité liées à l'utilisation des comptes, de surveiller et d'auditer les élévations de privilèges, et de désactiver ou révoquer les accès de manière sécurisée lorsqu'ils ne sont plus nécessaires.

1.4 Elle protège également les opérations de l'entreprise contre les erreurs opérationnelles ou les usages abusifs résultant d'accès excessifs ou non surveillés, et contribue à réduire le risque de fuite accidentelle de données, d'usage abusif de privilèges ou de non-conformité réglementaire.

2. Champ d'application

2.1 La présente politique s'applique à :

2.1.1 tous les employés, stagiaires, prestataires et utilisateurs tiers ayant accès aux systèmes d'information de l'organisation ;

2.1.2 tous les systèmes, équipements, services et plateformes gérés par l'organisation ou pour son compte, y compris les plateformes cloud, les infrastructures sur site et les outils tiers.

2.2 Elle couvre tous les types de comptes utilisateurs, y compris :

2.2.1 les comptes utilisateurs nominatifs (par exemple, comptes de messagerie, accès aux systèmes) ;

2.2.2 les comptes administrateur et les comptes système ;

2.2.3 les identifiants d'accès temporaires, invités ou tiers ;

2.2.4 les comptes de service utilisés par des applications ou des systèmes d'automatisation.

2.3 La politique s'applique à l'ensemble du cycle de vie des comptes, depuis la création et l'approbation jusqu'à la modification, la surveillance et la désactivation. Cela inclut l'attribution initiale des accès lors de l'intégration, les revues d'accès lors des changements de rôle et la révocation lors du départ.

3. Objectifs

3.1 Attribuer à tous les utilisateurs des systèmes des identifiants uniques et traçables, afin de garantir l'imputabilité et d'éliminer le partage d'identifiants.

3.2 Mettre en œuvre le principe du moindre privilège, afin que les utilisateurs ne reçoivent que le niveau minimal d'accès nécessaire à l'exercice de leurs fonctions.

3.3 Prévenir les accès non autorisés aux systèmes ou aux données sensibles au moyen de processus d'approbation et de revue clairement documentés.

3.4 Garantir la désactivation rapide des comptes utilisateurs lorsqu'ils ne sont plus nécessaires, par exemple en cas de départ, de fin de contrat ou de changement de rôle.

3.5 Maintenir un environnement sécurisé permettant de démontrer la conformité lors des audits, en documentant toutes les modifications de comptes, les approbations et les revues périodiques.

3.6 Garantir que l'élévation de privilèges est strictement contrôlée, approuvée de manière indépendante et journalisée, et que l'accès à privilèges est révoqué rapidement lorsqu'il n'est plus nécessaire.

4. Rôles et responsabilités

4.1 Directeur général (DG)

4.1.1 Assume la responsabilité globale de l'application de la présente politique.

4.1.2 Veille à ce que les pratiques de gestion des comptes soient alignées sur les exigences de certification ISO/IEC 27001 et les obligations légales applicables, notamment le RGPD.

4.1.3 Doit être informé sans délai de tout accès non autorisé, incident de sécurité ou manquement à la politique lié aux comptes utilisateurs.

4.1.4 Supervise les revues de la politique, les audits et les mesures d'application.

4.2 Responsable informatique ou prestataire externe de services informatiques

4.2.1 Est chargé de la mise en œuvre technique des contrôles relatifs aux comptes et aux privilèges sur les systèmes utilisés par l'organisation.

4.2.2 Ne peut attribuer, modifier et désactiver les comptes utilisateurs que sur la base d'approbations documentées.

4.2.3 Doit appliquer les exigences relatives à la complexité des mots de passe, au verrouillage automatique de l'écran, à l'authentification multifacteur (lorsqu'elle est disponible) et à la journalisation des systèmes.

4.2.4 Doit conserver des enregistrements sécurisés de toutes les approbations d'accès, de la propriété des comptes, des élévations de privilèges et des révocations.

4.2.5 Doit surveiller les comptes non autorisés ou orphelins et signaler tout écart au DG.

[... 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 La présente politique doit faire l'objet d'une revue au moins annuelle par le DG et le responsable informatique afin de garantir sa conformité avec :

9.1.1 les mesures de sécurité et orientations en vigueur de l'ISO/IEC 27001:2022 ;

9.1.2 les évolutions réglementaires (par exemple, RGPD, DORA, NIS2) ;

9.1.3 les changements affectant les systèmes, les services ou la structure de l'entreprise.

9.2 Des revues doivent également être menées après :

9.2.1 des incidents de sécurité significatifs ou des constats d'audit ;

9.2.2 des changements majeurs dans les systèmes informatiques ou l'architecture des comptes ;

9.2.3 l'introduction de nouvelles plateformes nécessitant une intégration du contrôle d'accès.

9.3 Toute modification doit être approuvée par le DG et communiquée clairement au personnel concerné.

10. Politiques associées et articulations

10.1 P2S – Politique relative aux rôles et responsabilités de gouvernance : établit les responsabilités et l'autorité décisionnelle pour les approbations d'accès et la supervision.

10.2 P4S – Politique de contrôle d'accès : encadre la mise en œuvre du contrôle d'accès à l'échelle des systèmes et les méthodes d'authentification.

10.3 P7S – Politique d'intégration et de départ : garantit que la création et la suppression des comptes sont intégrées aux changements de personnel gérés par les ressources humaines.

10.4 P8S – Politique de sensibilisation et de formation à la sécurité de l'information : forme les utilisateurs aux bonnes pratiques de sécurité relatives aux comptes et aux règles d'utilisation attendues.

10.5 P30S – Politique de réponse aux incidents : définit les actions à entreprendre si un usage abusif de compte conduit à un incident de sécurité ou à une divulgation non autorisée.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001

11.1.1 Clause 5.3 : exige que les rôles et responsabilités en matière de sécurité de l'information soient clairement attribués et appliqués.

11.1.2 Clause 8.1 : la planification et la maîtrise opérationnelle doivent inclure la gestion des accès utilisateurs.

11.2 ISO/IEC 27002

11.2.1 Mesure 8.2 : détaille les contrôles techniques et procéduraux relatifs à l'attribution, à la revue et à la suppression des privilèges élevés.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-2 : exige la création, la surveillance et la révocation des comptes sur la base de rôles et de processus définis.

11.3.2 AC-5 : traite de la séparation des tâches afin de prévenir les conflits ou les abus de privilèges.

11.3.3 AC-6 : impose l'application du principe du moindre privilège à l'ensemble des droits d'accès.

11.4 RGPD

11.4.1 Article 32 : exige des contrôles d'accès appropriés pour protéger les données à caractère personnel contre les accès non autorisés ou l'altération.

11.5 Directive NIS de l'UE

11.5.1 Article 21(2)(d) : impose la gestion des accès utilisateurs dans le cadre des contrôles de sécurité de base applicables aux entités essentielles et importantes.

11.6 Règlement DORA de l’UE

11.6.1 Article 9(2)(b) : exige des entités financières qu’elles mettent en œuvre des contrôles d’accès limitant et surveillant les droits à privilèges.

11.7 COBIT 2019

11.7.1 DSS05.03 : précise l’attribution et la suppression des accès utilisateurs dans le cadre de la gouvernance des systèmes d’information.

11.7.2 DSS05.04 : exige une revue continue des accès utilisateurs et leur alignement sur les rôles de l’organisation.