					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P04S					Titre du document : **Politique de contrôle d'accès P04S**							
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 5	
ISO/IEC 27002:2022	Mesures 5.15, 5.16, 5.17	
NIST SP 800-53 Rev. 5	AC-1 à AC-5	
RGPD de l'UE	Article 32	
NIS2 de l'UE	Article 21(2)(b)	
DORA de l'UE	Article 9	
COBIT 2019	APO07, DSS01	

1. Objet

1.1. La présente politique définit la manière dont l'organisation gère l'accès aux systèmes, aux données et aux installations afin de garantir que seules les personnes autorisées puissent accéder aux informations selon le besoin métier.

1.2. Elle établit des règles claires pour l'attribution, la modification, la surveillance et la suppression des accès utilisateurs, afin de réduire le risque d'accès non autorisé et de soutenir la conformité aux lois et normes applicables.

1.3. La politique impose l'application du principe du moindre privilège, en exigeant que les accès soient limités au strict minimum nécessaire à l'exercice des fonctions.

2. Champ d'application

2.1. La présente politique s'applique à toute personne qui utilise ou administre les accès aux systèmes d'information, aux réseaux, aux données ou aux installations de l'organisation, notamment :

2.1.1. Les employés

2.1.2. Les prestataires

2.1.3. Les travailleurs temporaires

2.1.4. Les prestataires externes de services informatiques

2.2. Elle couvre l'accès :

2.2.1. Aux applications de l'entreprise, aux partages de fichiers et aux bases de données

2.2.2. À la messagerie, au VPN et aux dispositifs d'accès à distance

2.2.3. Aux services cloud utilisés à des fins professionnelles

2.2.4. À l'accès physique aux zones sécurisées, telles que les bureaux ou les salles serveurs

2.3. La présente politique s'applique à l'ensemble des équipements (fournis par l'entreprise ou BYOD approuvé), des plateformes et des sites.

3. Objectifs

3.1. Garantir que les droits d'accès ne soient accordés qu'après une approbation formelle fondée sur le rôle et une justification métier.

3.2. Prévenir tout accès non autorisé ou excessif aux données sensibles, aux systèmes ou à l'infrastructure.

3.3. Définir des procédures claires pour l'attribution, la modification et la suppression des accès utilisateurs.

3.4. Exiger des revues d'accès régulières ainsi qu'une journalisation automatisée ou manuelle afin de répondre aux exigences d'audit.

3.5. Appuyer la mise en œuvre technique des restrictions d'accès au moyen de la configuration et de la surveillance.

4. Rôles et responsabilités

4.1. Directeur général

4.1.1. Approuve la présente politique et veille à la disponibilité des ressources nécessaires à la mise en œuvre de contrôles d'accès efficaces.

4.1.2. Approuve les dérogations et examine les audits annuels des accès.

4.2. Responsable informatique / prestataire informatique externe

4.2.1. Assure l'attribution, la modification et la suppression des comptes utilisateurs.

4.2.2. Tient un registre des contrôles d'accès consignant l'ensemble des activités (créations, modifications, suppressions).

4.2.3. Met en œuvre des contrôles d'accès fondés sur les rôles (RBAC) et impose une authentification forte (par exemple, MFA).

4.2.4. Analyse les journaux d'accès afin de détecter les activités suspectes et signale tout problème au Directeur général.

[... 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 de la politique

9.1.1. Le Responsable informatique doit revoir la présente politique chaque année. Toute évolution du contexte juridique, technique ou organisationnel doit entraîner une mise à jour immédiate.

9.2. Déclencheurs de revue

9.2.1. La politique doit également faire l'objet d'une revue si l'un des événements suivants se produit :

9.2.2. Des changements majeurs de systèmes ou des migrations vers le cloud

9.2.3. Des changements de rôles ou de structure organisationnelle

9.2.4. Un incident de sécurité impliquant un accès non autorisé

9.2.5. Des évolutions réglementaires (par exemple, mises à jour du RGPD, de NIS2 ou de DORA)

9.3. Documentation et communication des modifications

9.3.1. Les révisions doivent être consignées avec l'historique des versions, l'approbation du Directeur général et une communication à l'ensemble des personnes concernées.

9.4. Accessibilité et formation

9.4.1. La présente politique doit être mise à la disposition de l'ensemble du personnel, et une formation adaptée doit être dispensée lors de l'intégration puis annuellement.

10. Politiques connexes et articulations

10.1. La présente politique doit être appliquée en coordination avec les politiques SME suivantes afin d'assurer la mise en œuvre complète de pratiques d'accès sécurisées :

10.1.1. P3S – Politique d'utilisation acceptable : garantit que les utilisateurs comprennent les comportements acceptables dans le cadre des accès qui leur sont accordés.

10.1.2. P5S – Politique de gestion des changements : garantit que les droits d'accès sont alignés sur les changements de système approuvés.

10.1.3. P7S – Politique d'intégration et de départ : définit les points de déclenchement pour l'attribution et la suppression des accès utilisateurs.

10.1.4. P17S – Politique de protection des données et de la vie privée : garantit que les contrôles d'accès sont alignés sur les mesures de protection des données à caractère personnel.

10.1.5. P30S – Politique de réponse aux incidents : définit la manière dont les incidents liés aux accès (par exemple, usage abusif ou compromission) sont gérés et investigués.

11. Normes et référentiels de référence

11.1. ISO/IEC 27001

11.1.1. Clause 5.15 – Exige des politiques et processus de contrôle d'accès formalisés.

11.2. ISO/IEC 27002

11.2.1. Mesures 5.15 à 5.17 – Précisent des recommandations détaillées sur les accès fondés sur les rôles, la gestion du cycle de vie des utilisateurs et la gestion des accès à privilèges.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AC-1 à AC-5 – Exigent des politiques structurées pour la gestion des accès, y compris l'autorisation des comptes, la revue et la surveillance.

11.4. RGPD de l'UE

11.4.1. Article 32 – Exige des mesures techniques et organisationnelles (telles que la gestion des accès) pour garantir la sécurité et la confidentialité des données.

11.5. Directive NIS2 de l'UE

11.5.1. Article 21(2)(b) – Impose des contrôles d'accès opérationnels et des systèmes de gestion des identités afin de prévenir les accès non autorisés aux systèmes.

11.6. DORA de l'UE

11.6.1. Article 9 – Met l'accent sur la gestion sécurisée des risques liés aux TIC, y compris un contrôle d'accès robuste pour les entités financières.

11.7. COBIT 2019

11.7.1. APO07 – Sécurité gérée : appelle à des responsabilités d'accès définies et appliquées.

11.7.2. DSS01 – Gestion des opérations : inclut des procédures de gestion des accès logiques et de maintien d'environnements opérationnels sécurisés.