					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P04					Titre du document : **Politique de contrôle d'accès**							
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 5.15, 5.17, 5.18	Gestion des accès logiques et physiques
ISO/IEC 27002:2022	Mesures 8.2, 8.3	Contrôle d'accès fondé sur les rôles et gestion des identités
NIST SP 800-53 Rev. 5	AC-1 à AC-20, IA-1 à IA-8	Contrôles des comptes et des accès, identité/authentification
RGPD de l'UE	Articles 5(1)(f), 32(1)(b) ; considérant 39	Protection des données et minimisation
NIS2 de l'UE	Article 21(2)(c–e)	Contrôle d'accès, authentification des utilisateurs et protection des actifs
DORA de l'UE	Articles 6, 9(2)	Accès aux TIC/utilisateurs et contrôle renforcé des tiers
COBIT 2019	APO07, BAI03, DSS01, DSS05, MEA03	Intégration, opérations, surveillance, conformité

1. Objet

1.1 La présente politique définit les principes, les responsabilités et les exigences de contrôle obligatoires applicables à la gestion des accès aux systèmes d'information, aux applications, aux installations physiques et aux actifs informationnels de l'organisation.

1.2 Elle impose que les accès soient accordés en fonction du besoin métier, de la fonction exercée et du niveau de risque, conformément aux principes du moindre privilège, du besoin d'en connaître et de la séparation des tâches.

1.3 La présente politique soutient la mise en œuvre de la clause 5.15 de l'ISO/IEC 27001:2022 et des mesures associées relatives aux accès logiques et physiques, à l'authentification des utilisateurs et à la gestion du cycle de vie des accès.

1.4 La présente politique constitue un fondement de la protection des ressources numériques et physiques contre tout usage non autorisé ou abusif, ainsi que contre toute compromission.

2. Champ d'application

2.1 La présente politique s'applique à tous les utilisateurs, systèmes et installations relevant du périmètre du SMSI, y compris :

2.1.1 Les salariés, prestataires, fournisseurs et personnels temporaires

2.1.2 Les infrastructures sur site, les systèmes hébergés dans le cloud et les environnements hybrides

2.1.3 L'ensemble des actifs de l'entreprise — matériels, logiciels, données et zones physiques sécurisées

2.1.4 Les accès logiques (par ex. systèmes, réseaux, applications, API) et les accès physiques (par ex. bâtiments, centres de données)

2.2 Elle encadre les accès sur l'ensemble du cycle de vie des identités et des interactions avec les ressources, depuis l'intégration et l'attribution des accès jusqu'aux changements de rôle et au départ.

2.3 La présente politique couvre également les contextes de type Bring Your Own Device (BYOD) et d'accès à distance, afin de garantir la cohérence des contrôles, quels que soient les lieux et les modèles de propriété des équipements.

3. Objectifs

3.1 Mettre en œuvre des contrôles d'accès sécurisés fondés sur les rôles, afin de soutenir l'intégrité opérationnelle et la conformité réglementaire.

3.2 Garantir que les droits d'accès sont dûment approuvés, surveillés et révoqués en temps utile.

3.3 Prévenir tout accès non autorisé, toute élévation de privilèges et tout maintien de droits d'accès obsolètes.

3.4 Soutenir les principes du Zero Trust en appliquant par défaut un refus d'accès, sauf approbation et justification explicites.

3.5 Fournir aux auditeurs et aux parties prenantes des garanties fondées sur des revues d'accès automatisées, étayées par des éléments probants, ainsi que sur l'application effective de la politique.

3.6 Intégrer le contrôle d'accès dans les processus métier, les événements du cycle de vie RH et les architectures techniques.

4. Rôles et responsabilités

4.1 Direction générale

4.1.1 Valide la politique de contrôle d'accès et veille à l'allocation de budgets et d'effectifs adaptés à sa mise en œuvre.

4.1.2 Examine les risques liés au contrôle d'accès lors des revues de direction et attribue les responsabilités au niveau stratégique.

4.2 RSSI / Responsable du SMSI

4.2.1 Est responsable du cadre de contrôle d'accès et veille à son alignement sur l'ISO/IEC 27001 et les normes associées.

4.2.2 Coordonne l'application de la politique, les tests de contrôle et le reporting des indicateurs de contrôle d'accès.

4.2.3 Supervise la modélisation des accès fondée sur les risques et surveille les défaillances systémiques des contrôles.

[... 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 Déclencheurs et fréquence de revue

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

9.1.1.1 Chaque année, ou

9.1.1.2 À la suite d'un changement majeur de l'infrastructure informatique, des exigences réglementaires ou du niveau de risque

9.1.1.3 Après des incidents révélant des faiblesses dans les contrôles d'accès

9.1.1.4 En cas d'évolution significative des technologies d'authentification ou des plateformes d'identité

9.2 Autorité et processus de revue

9.2.1 Le RSSI ou le responsable désigné du SMSI gère le cycle de revue en intégrant :

9.2.1.1 Les constats de l'audit interne

9.2.1.2 Les résultats et indicateurs des revues d'accès

9.2.1.3 Les évolutions juridiques et réglementaires

9.2.1.4 Les changements des plateformes technologiques

9.2.2 Toute modification doit être approuvée par la direction générale et communiquée à l'ensemble des parties prenantes.

9.2.3 Les utilisateurs concernés peuvent être tenus d'accuser à nouveau réception de la politique en cas de mise à jour substantielle.

9.3 Contrôle des versions et documentation

9.3.1 La version de référence doit être conservée dans le référentiel documentaire du SMSI avec les métadonnées suivantes :

9.3.1.1 Numéro de version et journal des modifications

9.3.1.2 Date d'entrée en vigueur et date de prochaine revue

9.3.1.3 Propriétaire et autorité d'approbation

9.3.1.4 Registres de diffusion et d'accusé de réception

9.3.2 Les versions remplacées doivent être archivées et accessibles pendant au moins 3 ans.

10. Politiques associées et articulations

10.1 La présente politique dépend fonctionnellement des documents suivants et doit être interprétée conjointement avec eux :

10.1.1 P01 – Politique de sécurité de l'information : définit l'engagement de l'organisation en matière de sécurité et les attentes de haut niveau relatives au contrôle d'accès.

10.1.2 P03 – Politique d'utilisation acceptable : fixe les règles de comportement applicables aux accès et la responsabilité des utilisateurs dans un usage responsable des systèmes.

10.1.3 P05 – Politique de gestion des changements : encadre la mise en œuvre et les tests sécurisés des modifications apportées aux configurations d'accès, aux rôles ou aux structures de groupes.

10.1.4 P07 – Politique d'intégration et de départ : encadre l'octroi initial et la révocation des droits d'accès en fonction des événements du cycle de vie des utilisateurs.

10.1.5 P11 – Politique de gestion des comptes utilisateurs et des privilèges : décline les contrôles au niveau des comptes et complète la présente politique par des règles techniques d'application des accès.

10.2 Ensemble, ces politiques constituent un cadre cohérent et opposable de gouvernance des accès à l'échelle des unités métier et des technologies.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001:2022 :

11.1.1 Clause 5.15 – Contrôle d'accès : la présente politique répond à l'exigence de maîtrise des accès à l'information et aux autres actifs associés, sur la base des exigences métier et de sécurité de l'information.

11.1.2 Clause 5.17 – Gestion des identités et clause 5.18 – Informations d'authentification : ces exigences sont mises en œuvre au travers de l'attribution des identités, des mécanismes d'authentification et de l'affectation des privilèges.

11.1.3 Mesures de l'annexe A 8.2 (Contrôle d'accès) et 8.3 (Gestion des identités) : elles constituent le fondement des objectifs de contrôle de la présente politique, notamment l'accès fondé sur les rôles, l'intégration au cycle de vie des utilisateurs et la protection des accès à privilèges.

11.2 NIST SP 800-53 Rev. 5 :

11.2.1 Famille AC (AC-1 à AC-20) : la présente politique soutient les exigences NIST de contrôle d'accès applicables aux systèmes physiques et logiques, notamment la définition de la politique (AC-1), la gestion des comptes (AC-2) et la séparation des tâches (AC-5).

11.2.2 Famille IA (IA-1 à IA-8) : fournit des orientations relatives à l'authentification des identités, à la protection des identifiants et à la MFA.

11.2.3 AU-2, AU-12 : les exigences de journalisation et d'audit appliquées au titre de la présente politique soutiennent la traçabilité des actions des utilisateurs et l'investigation des incidents.

11.2.4 PE-2 à PE-6 : traitent des restrictions d'accès physique, que la présente politique applique partiellement au moyen des contrôles de badges et des autorisations d'accès aux bâtiments.

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

11.3.1 Article 5(1)(f) : les données à caractère personnel doivent être protégées contre tout accès non autorisé. La présente politique assure la mise en œuvre technique et procédurale de ce principe.

11.3.2 Article 32(1)(b) : impose la mise en œuvre de contrôles d'accès, de pseudonymisation et de chiffrement afin de prévenir tout traitement non autorisé des données à caractère personnel.

11.3.3 Considérant 39 : impose la minimisation des accès aux données à caractère personnel, appliquée ici au moyen du moindre privilège et des exigences de justification des accès.

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

11.4.1 Article 21(2)(c–e) : la présente politique permet la mise en œuvre de mesures techniques et organisationnelles de contrôle d'accès, d'authentification des utilisateurs et de protection des actifs au sein des entités essentielles et importantes.

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

11.5.1 Article 6 : impose des politiques de gestion des risques liés aux TIC incluant explicitement la gestion des accès utilisateurs et les contrôles du cycle de vie des identités. La présente politique répond à cette exigence pour les secteurs financier et des services TIC.

11.5.2 Article 9(2) : la présente politique soutient l'application de contrôles d'accès robustes dans le cadre de la gestion des services TIC fournis par des tiers et au sein d'un même groupe.

11.6 COBIT 2019 :

11.6.1 APO07 – Managed Human Resources : impose des contrôles d'intégration et de départ afin de soutenir la gouvernance des accès.

11.6.2 BAI03 – Managed Solutions Identification and Build : intègre les exigences de contrôle d'accès dans la conception des systèmes et les processus de changement.

11.6.3 DSS01 – Managed Operations et DSS05 – Managed Security Services : encadrent l'application des restrictions d'accès logique et la surveillance des violations.

11.6.4 MEA03 – Monitor, Evaluate, and Assess Compliance : soutient les mécanismes d'audit et d'assurance visant à valider l'efficacité du contrôle d'accès.