					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P11					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 6.1.3, 8	-
ISO/IEC 27002:2022	Contrôles 5.15-5.18	-
NIST SP 800-53 Rev.5	AC-1, AC-2, AC-5, AC-6, IA-2 à IA-5, AU-2, AU-12	-
RGPD de l'UE	Articles 5(1)(f), 32 ; considérant 39	-
NIS2 de l'UE	Articles 21(2)(a, d), 21(3)	-
DORA de l'UE	Articles 5, 9	-
COBIT 2019	DSS01, DSS05, APO13	-

1. Objet

1 La présente politique définit les contrôles obligatoires applicables à la gestion des comptes utilisateurs et des privilèges dans l'ensemble des systèmes d'information et services. Elle exige que l'accès aux ressources de l'organisation soit accordé sur la base d'une identité validée, d'un besoin lié au rôle et des principes de moindre privilège et de séparation des tâches.

1.1 Elle soutient l'engagement de l'organisation en matière de sécurité de l'information par la mise en œuvre de processus structurés et auditables pour le provisionnement des accès, l'attribution des privilèges, la surveillance des usages et la révocation des accès.

1.2 Cette politique est essentielle pour réduire les risques d'accès non autorisé, d'usage abusif des privilèges, de menace interne et de non-conformité aux cadres réglementaires applicables.

2. Champ d'application

2.1 La présente politique s'applique à l'ensemble du personnel, aux sous-traitants, aux prestataires tiers, aux consultants et à toute autre personne disposant d'un accès aux ressources informatiques, aux applications ou aux données de l'organisation.

2.2 Elle régit tous les systèmes et environnements dans lesquels des mécanismes d'authentification des utilisateurs et de contrôle d'accès sont mis en œuvre, y compris, sans s'y limiter :

2.2.1 les applications d'entreprise et les bases de données ;

2.2.2 les plateformes cloud et les environnements SaaS ;

2.2.3 les systèmes d'exploitation et les consoles d'administration ;

2.2.4 les outils d'accès à distance et les réseaux privés virtuels (VPN) ;

2.2.5 les systèmes de gestion des identités et des accès (IAM).

2.3 La politique couvre à la fois les comptes utilisateurs standard et les comptes à privilèges, et inclut des contrôles relatifs à :

2.3.1 la création, la modification et la désactivation des comptes ;

2.3.2 l'élévation de privilèges et la délégation ;

2.3.3 le contrôle et la surveillance des sessions ;

2.3.4 les méthodes d'authentification et la gestion des informations d'authentification.

3. Objectifs

3.1 Garantir que tous les comptes utilisateurs sont identifiables de manière unique, dûment autorisés et attribués uniquement après validation formelle du besoin.

3.2 Mettre en œuvre les principes de moindre privilège et prévenir les accès inutiles ou excessifs en imposant des contrôles stricts sur l'attribution et l'utilisation des comptes à privilèges.

3.3 Exiger une mise à jour en temps utile du statut des comptes en fonction des changements d'emploi ou de rôle, y compris une désactivation immédiate en cas de départ.

3.4 Permettre la détection proactive et la remédiation des comptes dormants, utilisés de manière abusive ou non autorisés au moyen de la journalisation, des revues et de l'automatisation.

3.5 Maintenir l'alignement sur l'ISO/IEC 27001:2022 et les normes associées, et satisfaire aux obligations prévues par les cadres juridiques et réglementaires pertinents tels que le RGPD, NIS2, DORA et COBIT 2019.

4. Rôles et responsabilités

4.1 Responsable de la sécurité des systèmes d'information (RSSI)

4.1.1 Est responsable de la présente politique et veille à son application dans l'ensemble de l'organisation.

4.1.2 Examine et approuve toute dérogation formelle ou tout cas d'accès d'urgence.

4.1.3 Rend compte des constats d'audit liés aux comptes et escalade les risques auprès de la haute direction.

4.2 Responsable du contrôle d'accès / administrateur informatique

4.2.1 Maintient et exploite les contrôles techniques liés à la gestion du cycle de vie des accès utilisateurs.

4.2.2 Exécute les actions de provisionnement, de suppression des accès et de gestion des privilèges sur la base d'une demande approuvée.

4.2.3 Tient à jour un registre de référence de tous les comptes utilisateurs, de leur statut et de leur niveau de privilège.

4.2.4 Appuie les audits et les revues de conformité au moyen des journaux et des rapports d'activité.

[... 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 être revue au moins une fois par an ou en cas de changements significatifs affectant :

9.1.1 la structure organisationnelle ou les processus métier ;

9.1.2 les systèmes informatiques, les plateformes d'identité ou les méthodes d'accès ;

9.1.3 les exigences réglementaires ou contractuelles relatives à la gestion des identités et des accès.

9.2 Le responsable de la sécurité des systèmes d'information (RSSI), conjointement avec le responsable du contrôle d'accès, est chargé d'initier le processus de revue et de coordonner les retours des parties prenantes.

9.3 Des revues intermédiaires peuvent être déclenchées par :

9.3.1 des incidents de sécurité liés à l'usage abusif de comptes ;

9.3.2 des constats d'audit mettant en évidence des défaillances dans la gestion du cycle de vie des accès ;

9.3.3 le déploiement de nouveaux outils de gestion des identités ou de gestion des accès à privilèges (PAM).

9.4 Les mises à jour de la présente politique doivent être :

9.4.1 soumises à gestion des versions et enregistrées dans la bibliothèque documentaire du SMSI ;

9.4.2 communiquées à toutes les parties prenantes concernées, y compris les chefs de département, les opérations informatiques et les RH ;

9.4.3 accompagnées de supports de formation et de guides de procédure mis à jour.

9.5 Toute modification doit être approuvée par la haute direction ou le comité de pilotage de la sécurité de l'information (ISSC) et journalisée à des fins d'audit.

10. Politiques associées et articulations

10.1 La présente politique est liée sur le plan opérationnel aux politiques associées suivantes du corpus du SMSI et s'appuie sur elles :

10.1.1 P4 Politique de contrôle d'accès : établit les principes et mécanismes généraux de contrôle d'accès, y compris les contrôles fondés sur des règles et sur les rôles.

10.1.2 P7 Politique d'intégration et de départ : définit les étapes procédurales d'ouverture et de clôture des accès utilisateurs en cohérence avec les actions RH.

10.1.3 P8 Politique de sensibilisation et de formation à la sécurité de l'information : renforce les responsabilités des utilisateurs en matière de sécurité des comptes et de protection des identifiants.

10.1.4 P13 Politique de classification et d'étiquetage des données : oriente les niveaux d'accès selon la classification des données, afin de garantir que les limites de privilèges sont alignées sur les niveaux de sensibilité.

10.1.5 P22 Politique de journalisation et de surveillance : garantit que la traçabilité d'audit est collectée pour toutes les activités liées aux comptes et revue afin de détecter les anomalies ou les usages non autorisés.

10.1.6 P30 Politique de réponse aux incidents : régit l'escalade, le confinement et les actions post-incident en cas d'usage abusif de privilèges ou d'activité non autorisée sur des comptes.

10.2 Chacune de ces politiques contribue, conjointement avec la présente politique, à l'application d'un cadre cohérent de gestion des identités et des accès fondé sur les risques à l'échelle de l'organisation.

11. Normes et référentiels de référence

11.1 La présente politique est alignée sur des normes de cybersécurité et des cadres réglementaires reconnus au niveau international, qui imposent une gestion sécurisée des identités, des accès et des privilèges comme composante essentielle de la sécurité de l'information de l'organisation.

11.2 ISO/IEC 27001:

11.2.1 Clause 6.1.3 - exige que les organisations déterminent, évaluent et traitent les risques de sécurité de l'information, ce qui fait de la gestion des accès et des privilèges un contrôle formel fondé sur les risques intégré au processus de planification du SMSI.

11.2.2 Clause 8.1 - Planification et maîtrise opérationnelles : renforce la mise en œuvre de mesures de protection techniques et procédurales encadrant l'accès des utilisateurs et les accès à privilèges.

11.3 ISO/IEC 27002:2022 - Contrôles 5.15 à 5.18 :

11.3.1 Contrôle 5.15 - Gestion des accès utilisateurs : soutient les processus formels de provisionnement des accès, d'autorisation d'accès et de revue périodique des droits d'accès.

11.3.2 Contrôle 5.16 - Gestion des identités : établit le caractère unique des identités, les contrôles de cycle de vie et l'application d'une authentification sécurisée.

11.3.3 Contrôle 5.17 - Informations d'authentification : garantit que l'attribution, la gestion et l'utilisation des informations d'authentification sont strictement contrôlées, traçables et alignées sur les exigences de sécurité tout au long du cycle de vie du compte utilisateur.

11.3.4 Contrôle 5.18 - Droits d'accès : est pleinement couvert par les exigences relatives à l'attribution des privilèges fondée sur les rôles, à l'audit et à l'approbation des accès élevés.

11.4 Ces contrôles guident la mise en œuvre structurée de l'enregistrement et de la suppression des comptes, de la séparation des privilèges et de l'utilisation des informations d'authentification. La présente politique impose une gouvernance du cycle de vie des identités, l'accès juste-à-temps et la surveillance des sessions élevées afin d'empêcher toute utilisation non autorisée des systèmes.

11.5 NIST SP 800-53 Rev.5:

11.5.1 AC-1 (Politique de contrôle d'accès) et AC-2 (Gestion des comptes) : couverts par les exigences de la politique en matière d'approbation des accès, de correspondance des rôles et d'audit des comptes utilisateurs.

11.5.2 AC-5 (Séparation des tâches) et AC-6 (Moindre privilège) : satisfaits par la restriction des privilèges, l'alignement sur les rôles professionnels et la double approbation pour les tâches à haut risque.

11.5.3 IA-2 à IA-5 (Identification et authentification) : appliqués au moyen de mécanismes d'authentification forte, de règles de cycle de vie des identifiants et d'exigences d'authentification multifacteur.

11.5.4 AU-2, AU-12 (Journalisation d'audit et analyse) : couverts par l'enregistrement des sessions et la surveillance des activités à privilèges dans les environnements sensibles.

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

11.6.1 Article 32 - Sécurité du traitement : exige des contrôles d'accès et des mécanismes de vérification d'identité pour protéger les données à caractère personnel. Cette exigence est satisfaite par l'approbation des comptes, les revues de privilèges et des mesures de protection d'authentification forte.

11.6.2 Article 5(1)(f) - Intégrité et confidentialité : garantit que les données à caractère personnel sont accessibles uniquement par des utilisateurs autorisés exerçant des rôles légitimes, exigence renforcée par l'application de la gestion des comptes.

11.6.3 Considérant 39 : appelle à une limitation claire des accès et à la responsabilisation ; la présente politique assure une traçabilité complète des identités utilisateurs et de l'attribution des privilèges.

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

11.7.1 Article 21(2)(a, d) : exige que les entités appliquent des politiques de gestion des accès et un traitement sécurisé de l'information relatif aux identifiants et aux sessions à privilèges, au moyen des contrôles de provisionnement des accès, de surveillance et d'exception prévus par la présente politique.

11.7.2 Article 21(3) : promeut la discipline d'accès et un niveau élevé d'assurance de l'identité dans les secteurs critiques, exigence satisfaite par l'usage d'identifiants uniques, du contrôle d'accès fondé sur les rôles (RBAC) et d'accès élevés limités dans le temps.

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

11.8.1 Article 5 - Gouvernance et contrôle des TIC : impose des processus formalisés de gestion des utilisateurs des TIC, couverts par le provisionnement des accès documenté, la désactivation et la gestion des exceptions.

11.8.2 Article 9 - Gestion des risques liés aux TIC : impose aux organisations de sécuriser les systèmes au moyen de restrictions d'accès et de surveillance, exigence couverte par l'authentification multifacteur, la journalisation des accès à privilèges et les revues centralisées.

11.9 COBIT 2019:

11.9.1 DSS01 - Opérations gérées : promeut l'application de contrôles opérationnels standardisés, y compris la gestion du cycle de vie des comptes utilisateurs et la documentation des accès.

11.9.2 DSS05 - Gestion des services de sécurité : reflète l'administration sécurisée des privilèges utilisateurs et systèmes, en soutenant l'atténuation des risques au moyen du moindre privilège et la validation de la piste d'audit.

11.9.3 APO13 - Sécurité gérée : exige une gouvernance des accès sur les actifs numériques, mise en œuvre au moyen de pratiques formalisées d'autorisation des comptes et des rôles, assorties d'exigences de revue périodique.