Politique de gestion des comptes utilisateurs

Référence	Version	Date	Catégorie
POL-VMS-002	v1.0	Mars 2025	Exploitation VMS & Vidéosurveillance

La gestion rigoureuse des comptes utilisateurs est un pilier fondamental de la sécurité d'un système de vidéoprotection. Cette politique définit les règles de création, de maintien et de suppression des comptes utilisateurs, ainsi que les principes d'attribution des droits d'accès, dans le respect du RGPD et des bonnes pratiques de cybersécurité.

---

01. Création de compte

Toute création de compte utilisateur sur le VMS est soumise à une demande formelle adressée au Responsable Sécurité, accompagnée d'une justification du besoin d'accès. Le Responsable Sécurité valide la demande avant que l'administrateur système procède à la création effective du compte.

Le principe du moindre privilège s'applique à chaque compte créé : les droits attribués sont strictement limités à ceux nécessaires à l'exercice des missions de l'utilisateur. Il est interdit d'attribuer par défaut des droits d'administration à un compte opérateur, même temporairement.

Un email de bienvenue est envoyé à l'utilisateur lors de la création de son compte. Cet email contient un lien de définition de mot de passe valide pendant 24 heures, les règles de sécurité applicables et un rappel des obligations liées à l'accès au système de vidéoprotection.

---

02. Convention de nommage des comptes

Les identifiants de compte suivent une convention standardisée : initiale du prénom suivie du nom de famille en minuscules (exemple :

jdupont). En cas de doublon, un chiffre est ajouté en suffixe (jdupont2). Cette convention facilite l'audit des journaux et l'identification immédiate de l'utilisateur associé à chaque action.

Les comptes de service (utilisés par des applications ou des intégrations automatisées) suivent la convention svc-[nom-application] et doivent faire l'objet d'une documentation spécifique précisant leur usage, leur propriétaire et les droits associés. Ils ne peuvent pas être utilisés pour des connexions interactives.

---

03. Durée de vie des comptes et désactivation automatique

Les comptes utilisateurs sont désactivés automatiquement après 90 jours consécutifs d'inactivité. Une notification est envoyée à l'utilisateur et à son responsable hiérarchique 15 jours avant la désactivation afin de permettre une réactivation justifiée si le besoin d'accès persiste.

Les comptes des personnels ayant quitté l'organisation (départ, mutation, fin de contrat) doivent être désactivés dans un délai maximum de 24 heures suivant la notification de départ. La suppression définitive du compte intervient après 30 jours de désactivation, une fois confirmée l'absence de besoin de consultation des journaux associés.

Les comptes temporaires créés pour des prestataires extérieurs ou des auditeurs sont automatiquement désactivés à la date de fin de mission indiquée lors de leur création. Cette date est obligatoire et ne peut excéder 90 jours ; une prolongation nécessite une nouvelle validation du Responsable Sécurité.

---

04. Interdiction des comptes partagés

L'utilisation d'un compte partagé entre plusieurs personnes est strictement prohibée. Chaque utilisateur doit disposer de son propre compte nominatif afin de garantir la traçabilité individuelle des actions effectuées sur le système. Cette exigence s'applique sans exception, y compris pour les postes de supervision partagés.

Les postes de supervision mutualisés (écrans de contrôle permanents) doivent être configurés de façon à obliger chaque opérateur à s'authentifier individuellement lors de la prise de poste. Les sessions ne peuvent pas être laissées ouvertes entre deux relèves sans déconnexion explicite.

---

05. Audit périodique des comptes

Le Responsable Sécurité procède à une revue complète de la liste des comptes utilisateurs actifs tous les trimestres. Cette revue vise à identifier et désactiver les comptes devenus orphelins (départ non signalé), les comptes dont les droits ne correspondent plus aux fonctions actuelles et les comptes de service non documentés.

> **Les résultats de l'audit trimestriel sont consignés dans un rapport transmis à la Direction, précisant le nombre de comptes actifs, le nombre de comptes désactivés et les éventuelles anomalies détectées. Ce rapport constitue une pièce du dossier de conformité RGPD.**