Procédure d'accès aux enregistrements

Référence	Version	Date	Catégorie
PROC-RGPD-004	v1.1	Décembre 2024	RGPD & Conformité Vidéosurveillance

La gestion des accès aux enregistrements vidéo est un enjeu majeur de conformité RGPD et de sécurité opérationnelle. La présente procédure définit qui peut accéder aux enregistrements, dans quelles conditions et avec quelles garanties de traçabilité, afin de prévenir les accès abusifs et de démontrer la maîtrise du traitement en cas de contrôle.

---

01. Personnes habilitées à consulter les enregistrements

L'accès aux enregistrements vidéo est strictement réservé aux personnes désignées par le responsable de traitement et formellement habilitées à cette fin. La liste des personnes habilitées est tenue à jour par le responsable de la sécurité ou le DPO. Elle précise, pour chaque personne : son nom, sa fonction, le périmètre de caméras accessible (toutes ou sous-ensemble), le niveau d'accès (visualisation temps réel, consultation des archives, extraction) et la durée de validité de l'habilitation.

Les catégories de personnes pouvant être habilitées incluent : le responsable de la sécurité, les agents de sûreté ou de sécurité en poste, le DPO pour les besoins de contrôle interne, la direction générale pour les incidents majeurs, et les techniciens de Mileo Technology dans le strict cadre des opérations de maintenance. Aucun accès ne peut être accordé à des personnes extérieures à ces catégories sans décision formelle du responsable de traitement.

---

02. Traçabilité des consultations

Toute consultation d'enregistrements doit être tracée dans le système de journalisation du VMS ou du NVR. Le journal d'accès enregistre a minima : l'identifiant de la personne ayant accédé, l'horodatage de connexion et de déconnexion, les caméras et plages horaires consultées, le type d'opération réalisée (visualisation, export, suppression). Cette journalisation est automatique sur les plateformes VMS conformes ; pour les systèmes moins sophistiqués, un registre manuel est tenu.

Le journal d'accès est protégé contre toute modification ou suppression par les utilisateurs ordinaires. Seul l'administrateur système peut y accéder, et ses propres accès sont eux-mêmes tracés par un mécanisme distinct. L'intégrité des journaux est vérifiée lors des audits périodiques.

---

03. Restrictions d'accès selon les rôles

Le principe du moindre privilège s'applique rigoureusement : chaque utilisateur n'accède qu'aux caméras et aux archives strictement nécessaires à l'exercice de ses fonctions. Un agent de sécurité affecté au hall d'entrée n'a pas accès aux enregistrements des zones de direction ou des bureaux. Un responsable de site peut avoir accès à l'ensemble des caméras de son site, mais pas aux caméras d'autres sites.

Les accès en temps réel (supervision live) et les accès aux archives (enregistrements passés) peuvent être accordés de façon distincte. Un opérateur de supervision peut avoir accès aux flux live sans avoir accès aux archives, limitant ainsi le risque d'extraction non autorisée d'enregistrements à des fins détournées.

---

04. Audit annuel des droits d'accès

Une revue complète des droits d'accès au système de vidéosurveillance est réalisée au minimum une fois par an. Cette revue vérifie que chaque compte actif correspond à une personne encore en fonction et habilitée, que les droits accordés sont conformes au rôle actuel de la personne (mobilité interne, évolution de poste), et qu'aucun compte orphelin (personne ayant quitté la société ou changé de poste) ne subsiste.

> **Les comptes des personnes ayant quitté l'organisation sont désactivés le jour de leur départ. Les comptes inactifs depuis plus de quatre-vingt-dix jours font l'objet d'une vérification et sont désactivés si l'inactivité n'est pas justifiée. Le résultat de l'audit annuel est consigné dans un compte rendu signé par le responsable de traitement et conservé cinq ans.**