Procédure d'export sécurisé des vidéos

Référence	Version	Date	Catégorie
PROC-VMS-006	v1.1	Avril 2025	Exploitation VMS & Vidéosurveillance

L'export d'enregistrements vidéo est une opération sensible dont chaque étape doit être rigoureusement encadrée pour garantir la légitimité de l'accès aux données, l'intégrité des extraits exportés et la traçabilité complète de l'opération. Cette procédure s'applique à tout export réalisé depuis le VMS, quel qu'en soit le motif.

---

01. Motifs légitimes d'export

L'export d'enregistrements vidéo n'est autorisé que dans les cas suivants : réquisition judiciaire ou demande formelle des forces de l'ordre, enquête interne sur un incident de sécurité avéré, démarche auprès d'une compagnie d'assurance dans le cadre d'un sinistre, ou demande d'exercice du droit d'accès d'une personne concernée au titre du RGPD.

Toute demande d'export doit être accompagnée d'une justification écrite précisant le motif, la plage temporelle concernée, les caméras impliquées et le destinataire final des données. Cette justification est conservée avec le registre des exports pendant 3 ans minimum.

---

02. Autorisation préalable obligatoire

Aucun export ne peut être réalisé sans l'autorisation écrite préalable du Responsable Sécurité. En cas d'indisponibilité de ce dernier, l'autorisation peut être délivrée par son délégué désigné. Les réquisitions judiciaires tiennent lieu d'autorisation automatique et doivent être transmises immédiatement au Responsable Sécurité.

L'autorisation doit être accordée avant le début de l'export. Les exports réalisés sans autorisation préalable, même a posteriori régularisés, constituent une violation de la présente procédure et font l'objet d'une déclaration d'incident dans le registre de conformité RGPD.

---

03. Format d'export et chiffrement

Les exports sont réalisés dans le format natif du VMS ou, sur demande expresse, dans un format ouvert (MP4) accompagné du lecteur propriétaire si nécessaire. L'extrait exporté est systématiquement accompagné d'un fichier de métadonnées précisant l'origine, la plage temporelle et l'empreinte cryptographique (hash SHA-256) de chaque fichier.

Lorsque l'export est destiné à des tiers externes (forces de l'ordre, assureurs, avocats), les fichiers sont chiffrés avec une clé symétrique AES-256 dont le mot de passe est transmis séparément du support physique, par canal sécurisé. Cette mesure garantit la confidentialité des données en transit.

---

04. Support physique sécurisé

L'export physique est réalisé sur un support dédié (clé USB ou DVD) fourni par l'organisation et réservé à cet usage. Les supports personnels et les plateformes de partage cloud non approuvées sont interdits. Le support est étiqueté avec le numéro de dossier, la date d'export et le niveau de confidentialité.

La remise du support à un tiers est effectuée en mains propres contre signature, ou par envoi postal recommandé avec accusé de réception. Toute remise donne lieu à un enregistrement dans le registre des exports précisant l'identité du destinataire, la date et le mode de remise.

---

05. Registre des exports et destruction sécurisée

Chaque export est enregistré dans le registre des exports du VMS, qui constitue également une entrée dans le registre des activités de

traitement au titre de l'article 30 du RGPD. Le registre est consultable à tout moment par le DPO et lors des contrôles de la CNIL.

> **Les supports temporaires ayant servi à la réalisation d'un export interne (copie de travail, support de duplication) sont détruits physiquement ou formatés de manière sécurisée (norme DoD 5220.22-M ou équivalent) dans les 48 heures suivant la finalisation de l'export. La destruction est consignée dans le registre des exports.**