Politique de sécurisation des exportations vidéo

Référence	Version	Date	Catégorie
POL-CYB-006	v1.0	Avril 2025	Cybersécurité

L'exportation d'images vidéo constitue un risque majeur pour la vie privée des personnes filmées et engage la responsabilité juridique du responsable de traitement. Que ce soit pour une remise aux autorités judiciaires, à un service d'investigation interne ou à une compagnie d'assurance, chaque export doit être réalisé avec le niveau de sécurité approprié. Mileo Technology encadre strictement ces opérations dans ses procédures et dans les formations dispensées à ses clients.

---

01. Chiffrement obligatoire des exports

Toute exportation de séquences vidéo doit être réalisée dans un format chiffré. Le chiffrement appliqué est AES-256 au minimum. Les NVR et VMS modernes proposent des exports natifs chiffrés avec lecteur dédié ; cette fonctionnalité est activée et configurée lors de la mise en service de chaque système.

Pour les équipements ne proposant pas d'export natif chiffré, les fichiers exportés sont immédiatement chiffrés après export, avant tout transfert ou remise. L'utilisation d'un outil de chiffrement certifié ou référencé par l'ANSSI est imposée. Les fichiers en clair sont supprimés de manière sécurisée après chiffrement.

---

02. Support physique sécurisé

Les exports destinés à être remis physiquement (clé USB, DVD) utilisent exclusivement des supports chiffrés matériellement ou des supports standards accompagnés d'un chiffrement logiciel fort. Les clés USB non chiffrées sont formellement interdites pour le transport d'images vidéo.

Le support physique est remis en main propre au destinataire autorisé, contre signature d'un accusé de réception précisant : date de remise, identité du remettant, identité du destinataire, contenu du support (dates, caméras, durée des séquences), objet de la remise. Cet accusé de réception est conservé 5 ans.

---

03. Traçabilité et destinataires autorisés

Chaque exportation est tracée dans un registre des extractions vidéo, distinct du journal d'événements du système. Ce registre consigne : date et heure de l'export, opérateur ayant réalisé l'export, plages horaires exportées, caméras concernées, format, destinataire et objet de la remise.

Seules les personnes expressément autorisées par le responsable du traitement (client) peuvent réaliser ou obtenir des exports vidéo. La liste des personnes autorisées est formalisée et maintenue à jour. Les demandes des autorités judiciaires ou policières font l'objet d'une vérification de l'habilitation avant toute remise.

---

04. Interdiction d'envoi par email non chiffré

L'envoi de séquences vidéo par email en clair (pièce jointe non chiffrée) est formellement interdit, quelle que soit la taille du fichier ou le caractère supposément privé de la messagerie. Un email peut être intercepté, redirigé ou stocké indéfiniment sur des serveurs tiers.

Si un transfert électronique est nécessaire, il doit utiliser une plateforme d'échange de fichiers sécurisée (chiffrement de bout en bout, authentification du destinataire, lien d'accès à durée limitée, notification de téléchargement). Mileo Technology recommande et peut mettre à disposition une telle solution pour ses clients.

---

05. Destruction des supports temporaires

Les supports ayant servi à un export vidéo temporaire (étape intermédiaire avant remise ou transfert) sont détruits ou effacés de manière sécurisée après l'opération. La suppression simple d'un fichier

ne suffit pas ; un effacement sécurisé (écrasement des données) est réalisé.

> **Les supports physiques obsolètes ou défectueux contenant des images vidéo sont détruits physiquement selon la norme DIN 66399 (niveau de sécurité adapté à la sensibilité des données). Un certificat de destruction est produit pour les destructions de supports de sites sensibles.**

Boulevard de Courcelles, 75008 Paris — hello@mileotech.com