# Politique cybersécurité installateur

| Référence | Version | Date | Catégorie |
|---|---|---|---|
| **POL-CYB-001** | v1.2 | Mai 2025 | Cybersécurité |

> ***Prioritaire***

Mileo Technology s'engage à intégrer la cybersécurité comme composante essentielle de chaque projet d'installation, de la conception à la maintenance. Cette politique définit les exigences minimales applicables à l'ensemble des systèmes déployés et des accès réalisés par nos équipes. Elle s'appuie sur le référentiel de l'ANSSI et s'inscrit dans une démarche de responsabilité vis-à-vis de nos clients.

---

## 01. Périmètre d'application

Cette politique s'applique à l'ensemble des équipements installés ou maintenus par Mileo Technology : caméras IP, enregistreurs NVR/DVR, serveurs VMS, contrôleurs d'accès, interphones IP, routeurs et commutateurs dédiés aux systèmes de sécurité.

Elle couvre également tous les accès distants réalisés par les techniciens et ingénieurs de Mileo Technology, qu'il s'agisse d'interventions de maintenance, de dépannage ou de supervision. Les sous-traitants mandatés par Mileo Technology sont soumis aux mêmes exigences, formalisées dans les contrats de prestation.

Les systèmes existants chez les clients, antérieurs à l'intervention de Mileo Technology, font l'objet d'une évaluation initiale et d'un plan de mise en conformité progressif, documenté et validé avec le client.

---

## 02. Référentiel et cadre réglementaire

Mileo Technology base sa politique cybersécurité sur les guides et recommandations publiés par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), notamment le guide de sécurisation des systèmes de vidéoprotection et les recommandations relatives à l'administration sécurisée des systèmes d'information.

Pour les clients soumis à la directive NIS2 (opérateurs d'importance vitale, entités essentielles et importantes), Mileo Technology adapte ses pratiques aux exigences renforcées de gestion des risques de cybersécurité imposées par cette directive, transposée en droit français.

La norme ISO 27001 constitue un référentiel de bonnes pratiques complémentaire, dont les contrôles pertinents sont intégrés dans nos procédures opérationnelles. Les exigences du RGPD relatives à la sécurité des données à caractère personnel (notamment les images des personnes) sont intégralement prises en compte.

---

## 03. Responsabilités

Le responsable technique de Mileo Technology est désigné référent cybersécurité. Il valide les politiques, suit les incidents, pilote les revues annuelles et assure la veille sur les menaces et vulnérabilités affectant les systèmes installés.

Chaque chef de projet est responsable de l'application de la politique cybersécurité sur les projets qu'il pilote. Il s'assure que la configuration des équipements respecte les standards définis et que la documentation de sécurité est complète à la remise du système.

Les techniciens sont responsables de l'application des procédures lors de chaque intervention. Ils sont formés annuellement aux exigences cybersécurité et signent un engagement de confidentialité et de respect des procédures.

---

## 04. Principes fondamentaux

Le principe de moindre privilège est appliqué systématiquement : chaque compte d'accès ne dispose que des droits strictement nécessaires à sa fonction. Les comptes administrateurs sont distincts des comptes d'exploitation courants.

La défense en profondeur guide l'architecture de chaque installation : segmentation réseau, authentification forte, chiffrement des communications, journalisation des accès et supervision active constituent des couches complémentaires de protection.

Tout équipement est configuré selon un durcissement (hardening) préalable à sa mise en service : suppression des comptes et services inutiles, désactivation des protocoles non sécurisés, activation du chiffrement des flux. Aucun équipement n'est mis en service avec sa configuration d'usine.

---

## 05. Revue et amélioration continue

Cette politique fait l'objet d'une revue annuelle formalisée, associant le référent cybersécurité, la direction et les chefs de projet. La revue intègre le bilan des incidents de l'année, les évolutions réglementaires et les nouvelles menaces identifiées.

Tout incident de sécurité significatif déclenche une revue extraordinaire et une mise à jour de la politique si nécessaire. Les enseignements tirés sont diffusés à l'ensemble des équipes techniques sous forme de bulletins internes.

> **Les indicateurs de performance cybersécurité (nombre de mises à jour firmware réalisées, délai moyen de correction des vulnérabilités, taux de conformité des configurations) sont suivis trimestriellement et présentés à la direction.**