Référentiel sûreté & cybersécurité client premium

Référence	Version	Date	Catégorie
STD-PREM-001	v2.0	Mars 2025	Documents Premium

> ***Premium***

Ce référentiel définit les niveaux de protection proposés par Mileo Technology à ses clients, les exigences techniques et organisationnelles associées à chaque niveau, et le cadre réglementaire applicable. Il constitue la base contractuelle des engagements de sécurité pour les clients ayant souscrit une offre de niveau Renforcé ou Premium.

---

01. Niveaux de protection

Le niveau Standard correspond aux exigences minimales applicables à tout système de sécurité électronique installé par Mileo Technology. Il inclut la conformité réglementaire de base (autorisation préfectorale pour la vidéoprotection, conformité RGPD des traitements), le changement des identifiants par défaut sur tous les équipements, la mise à jour des firmwares à la mise en service et une maintenance annuelle.

Le niveau Renforcé s'adresse aux organisations disposant d'actifs sensibles ou soumises à des obligations sectorielles renforcées (secteur bancaire, santé, collectivités). Il ajoute au niveau Standard la segmentation réseau dédiée (VLAN vidéo isolé), le chiffrement des flux de supervision, l'authentification forte pour l'accès aux systèmes de sécurité, et une maintenance semestrielle incluant un audit de configuration.

Le niveau Premium est conçu pour les OIV (Opérateurs d'Importance Vitale), les OSE (Opérateurs de Services Essentiels) et les organisations à très haute sensibilité. Il inclut toutes les exigences du niveau Renforcé, complétées par une architecture zéro-trust pour les accès

distants, un SIEM dédié à la supervision des événements de sécurité, des tests d'intrusion annuels, et un engagement contractuel de disponibilité avec SLA défini.

---

02. Exigences techniques par niveau

La segmentation réseau est obligatoire à partir du niveau Renforcé : les équipements de vidéosurveillance et de contrôle d'accès doivent être isolés sur un VLAN dédié, sans accès direct à Internet. Les flux de management (accès administration) et les flux vidéo (streaming) sont séparés sur des sous-réseaux distincts. Au niveau Premium, une DMZ est mise en œuvre pour les accès distants légitimes.

Le chiffrement des communications est exigé sur l'ensemble des niveaux mais avec des périmètres progressifs : Standard (chiffrement des accès web d'administration en HTTPS), Renforcé (chiffrement de tous les flux de supervision et des connexions aux NVR), Premium (chiffrement de bout en bout incluant les flux RTSP via TLS, les exports de vidéos et les communications entre composants du VMS).

La gestion des accès distants fait l'objet d'exigences strictes dès le niveau Renforcé : VPN avec authentification multi-facteurs obligatoire, journalisation de toutes les connexions avec conservation pendant 12 mois, revue trimestrielle des droits d'accès distants. Au niveau Premium s'ajoute l'obligation d'un bastion d'accès centralisé avec enregistrement des sessions.

---

03. Exigences réglementaires

Le RGPD s'applique à l'ensemble des niveaux dès lors que le système traite des données à caractère personnel (images de personnes physiques identifiables). Les obligations comprennent la tenue d'un registre des traitements, la désignation d'un DPO si applicable, la réalisation d'une analyse d'impact (AIPD) pour les traitements à risque élevé, le respect des durées de conservation légales (7 jours en principe pour la vidéosurveillance en lieu de travail selon la CNIL), et l'information des personnes concernées.

La directive NIS2, transposée en droit français par la loi du 26 mars 2024, impose aux OIV et OSE des obligations renforcées en matière de

gestion des risques cyber, de notification des incidents, de sécurité de la chaîne d'approvisionnement et de formation des dirigeants. Les clients soumis à NIS2 se voient proposer un accompagnement spécifique dans le cadre de l'offre Premium, incluant la documentation de conformité et l'assistance lors des contrôles de l'ANSSI.

---

04. Exigences organisationnelles

Quelle que soit le niveau, les intervenants Mileo Technology affectés au site doivent avoir suivi les formations de sensibilisation obligatoires (RGPD, cybersécurité) et détenir les habilitations requises par le site. Au niveau Premium, les intervenants font l'objet d'un contrôle de casier judiciaire systématique et sont soumis à une procédure d'accréditation nominative par le client.

> **Les clients de niveau Renforcé et Premium doivent désigner un référent sécurité interne, interlocuteur de Mileo Technology pour la gestion des incidents et des mises à jour. Des exercices de gestion de crise cyber sont proposés annuellement aux clients Premium, permettant de tester les procédures de réponse à incident et de réduction des délais de reprise d'activité.**

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