Manuel de gouvernance sécurité Mileo Technology

Référence	Version	Date	Catégorie
MAN-PREM-001	v1.2	Avril 2025	Documents Premium

> ***Premium***

Ce manuel décrit l'organisation et les pratiques de gouvernance de la sécurité au sein de Mileo Technology. Il a vocation à démontrer à nos clients et partenaires que nous appliquons à notre propre organisation les exigences que nous leur recommandons. La sécurité de nos systèmes internes, de nos données et de nos processus est la première condition de la confiance que nos clients nous accordent.

---

01. Organisation de la gouvernance sécurité

La gouvernance de la sécurité chez Mileo Technology repose sur un comité de sécurité réuni trimestriellement, présidé par la direction générale et composé du Responsable de la Sécurité des Systèmes d'Information (RSSI), du Délégué à la Protection des Données (DPO) et des responsables opérationnels. Ce comité examine l'état des risques, valide les décisions structurantes et arbitre les investissements en matière de sécurité.

Le RSSI est garant de la politique de sécurité des systèmes d'information et de son application. Il conduit les analyses de risques, supervise les audits techniques, pilote les plans de remédiation et est le point de contact privilégié en cas d'incident de sécurité. Le DPO assure la conformité au RGPD et à la réglementation applicable aux traitements de données à caractère personnel, tant pour les traitements internes que pour les traitements réalisés pour le compte des clients.

---

02. Processus de revue des risques

Une analyse des risques formalisée selon la méthode EBIOS Risk Manager est conduite annuellement. Elle couvre les risques pesant sur les systèmes d'information internes (GMAO, ERP, messagerie, outils de supervision), sur les données clients hébergées ou traitées, et sur les systèmes de nos clients auxquels nos collaborateurs ont accès dans le cadre de leurs missions.

Les risques identifiés sont consignés dans un registre des risques maintenu à jour en continu. Chaque risque est qualifié par sa vraisemblance et son impact, et associé à un ou plusieurs traitements (acceptation, réduction, transfert, évitement). Le registre est présenté au comité de sécurité à chaque réunion trimestrielle.

---

03. Indicateurs de maturité sécurité

La maturité de la sécurité chez Mileo Technology est mesurée à travers un tableau de bord mensuel comprenant notamment : le taux de mise à jour des équipements et logiciels (cible : 100 % dans les 30 jours suivant la disponibilité d'un correctif critique), le taux de couverture des collaborateurs par les formations de sensibilisation (cible : 100 % par an), le délai moyen de détection et de traitement des incidents de sécurité, et le score de maturité issu de l'auto-évaluation annuelle selon le cadre CIS Controls.

Ces indicateurs sont communiqués à la direction générale dans un rapport mensuel synthétique. Leur évolution dans le temps est analysée lors des comités de sécurité pour identifier les tendances et ajuster les priorités du plan d'amélioration.

---

04. Plan d'amélioration continue

Sur la base des résultats de l'analyse des risques et des indicateurs de maturité, un plan d'amélioration de la sécurité est défini annuellement. Il est structuré en actions prioritaires (P1 : à réaliser dans le mois), normales (P2 : dans le trimestre) et différées (P3 : dans l'année), chacune associée à un responsable, un budget et une date de livraison.

Le suivi de l'avancement des actions est intégré à l'ordre du jour de chaque comité de sécurité. Les actions non réalisées dans les délais prévus font l'objet d'une analyse des causes et d'un ajustement du plan. La clôture formelle d'une action requiert la validation du RSSI sur la base d'éléments probants (rapport d'audit, test de pénétration, capture d'écran de configuration).

---

05. Communication envers les clients

Mileo Technology s'engage à informer ses clients de tout incident de sécurité susceptible d'affecter leurs données ou leurs systèmes dans un délai de 72 heures suivant la prise de connaissance de l'incident, conformément aux obligations du RGPD. La notification comprend une description de l'incident, les catégories de données ou de systèmes concernés, les mesures prises immédiatement et le plan de remédiation.

> **Au-delà des obligations légales, Mileo Technology publie un rapport de transparence annuel résumant les incidents significatifs de l'année écoulée (anonymisés), les évolutions de la posture de sécurité et les engagements pour l'exercice suivant. Ce rapport est transmis aux clients sous accord cadre et disponible sur demande pour les autres clients.**

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