Politique de confidentialité interne

Référence	Version	Date	Catégorie
POL-GOV-002	v1.2	Janvier 2025	Gouvernance & Éthique

> ***Prioritaire***

La politique de confidentialité interne de Mileo Technology établit le cadre de classification, de traitement et de protection des informations au sein de l'entreprise. Elle s'applique à toutes les données générées, reçues ou traitées dans le cadre des activités professionnelles, quel que soit leur support.

---

01. Classification des informations

Mileo Technology applique un système de classification à trois niveaux. Le niveau « Public » couvre les informations destinées à être communiquées librement : plaquettes commerciales, références clients publiées avec accord, actualités de l'entreprise. Le niveau « Sensible » regroupe les informations à usage interne restreint : propositions commerciales, configurations techniques, données RH non nominatives. Le niveau « Confidentiel » désigne les informations à accès strictement limité : contrats clients, données personnelles, identifiants d'accès, plans de sites sécurisés.

Chaque collaborateur est responsable de la classification correcte des documents qu'il produit. En cas de doute, le niveau supérieur s'applique par défaut. Les documents multi-niveaux (rapport incluant des données confidentielles et des éléments publics) sont classifiés au niveau le plus élevé qu'ils contiennent.

Les documents classifiés « Confidentiel » doivent porter une mention explicite en en-tête et en pied de page. Leur diffusion est tracée et limitée aux personnes ayant un besoin opérationnel avéré d'y accéder, selon le principe du moindre privilège.

---

02. Règles de stockage et de partage

Les documents sensibles et confidentiels doivent être stockés exclusivement sur les espaces de stockage approuvés par Mileo Technology : serveur de fichiers interne, espace cloud d'entreprise chiffré. Le stockage sur des supports personnels, clés USB non chiffrées ou services cloud grand public (Google Drive personnel, Dropbox) est interdit.

Le partage de documents confidentiels avec des tiers (clients, sous-traitants, partenaires) doit se faire via des canaux sécurisés : espace client dédié, lien à durée limitée avec authentification, ou remise en main propre contre signature. L'envoi par email non chiffré de documents contenant des données personnelles ou des configurations techniques est prohibé.

Les droits d'accès aux espaces de stockage partagés sont accordés nominativement et révisés trimestriellement. Tout accès non justifié par les besoins opérationnels est révoqué. Les départs de collaborateurs entraînent la révocation immédiate de tous les accès le jour de la fin de contrat.

---

03. Emails et communication externe

La messagerie professionnelle Mileo Technology est l'unique canal autorisé pour les communications professionnelles avec l'extérieur. L'usage de messageries personnelles pour des échanges professionnels est interdit, même pour des communications a priori anodines, car il compromet la traçabilité et la sécurité des échanges.

Les pièces jointes contenant des informations classifiées « Confidentiel » envoyées à l'extérieur doivent être protégées par un mot de passe transmis via un canal distinct (SMS, appel téléphonique). Pour les documents particulièrement sensibles, le recours à une solution de partage sécurisé avec authentification du destinataire est obligatoire.

Toute communication externe au nom de Mileo Technology engage l'entreprise. Les collaborateurs veillent à ce que leurs échanges écrits soient factuels, mesurés et exempts de toute information susceptible d'être mal interprétée ou de nuire à l'image de l'entreprise ou d'un tiers.

---

04. Droit à l'oubli en interne et durées de conservation

Mileo Technology applique le principe de minimisation des données à ses propres traitements internes. Les informations personnelles relatives aux collaborateurs (dossiers RH, évaluations, données de santé) sont conservées selon les durées légales applicables et supprimées dès que ces durées sont échues, sauf obligation légale de conservation prolongée.

Les données de prospection commerciale (contacts non convertis en clients) sont conservées au maximum trois ans à compter du dernier contact, conformément aux recommandations de la CNIL. Les données clients actifs sont conservées pendant toute la durée de la relation contractuelle et cinq ans après son terme pour répondre aux obligations légales et aux éventuels litiges.

Un calendrier de conservation est tenu à jour par le référent données de l'entreprise. Des purges automatiques ou semi-automatiques sont programmées pour les catégories de données dont la durée de conservation est définie. Tout collaborateur peut solliciter la suppression d'informations le concernant en dehors des délais légaux en adressant une demande motivée au référent données.

---

05. Gestion des incidents de confidentialité

Tout incident susceptible de compromettre la confidentialité d'informations internes ou clients (perte d'un support, accès non autorisé constaté, envoi à un mauvais destinataire) doit être déclaré sans délai au responsable informatique et au référent données. La dissimulation d'un incident constitue une faute grave.

Les incidents impliquant des données à caractère personnel font l'objet d'une procédure de notification conforme à l'article 33 du RGPD : évaluation de la gravité, notification à la CNIL dans les 72 heures si le risque est avéré, information des personnes concernées si le risque est élevé. Un

> **registre des incidents est tenu et audité annuellement.**

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