Politique d'utilisation des équipements personnels

Référence	Version	Date	Catégorie
POL-INT-001	v1.0	Mars 2025	Sécurité des Interventions Terrain

La sécurité des systèmes d'information de nos clients exige que les techniciens Mileo Technology n'utilisent que des équipements professionnels maîtrisés lors de leurs interventions. Cette politique définit les règles d'utilisation des équipements sur les sites clients et précise les équipements fournis par l'entreprise pour chaque type d'intervention. Son respect protège nos clients contre les risques de fuite de données et de compromission de leurs systèmes.

---

01. Interdiction du BYOD sur les installations clients

Le BYOD (Bring Your Own Device — utilisation d'équipements personnels à des fins professionnelles) est strictement interdit sur l'ensemble des installations clients de Mileo Technology. Cette interdiction couvre tous les types d'équipements personnels : ordinateurs portables, tablettes, smartphones, clés USB, disques durs externes, outils de diagnostic connectés, multimètres intelligents ou tout autre dispositif susceptible d'établir une connexion avec le réseau ou les équipements du client.

Cette interdiction se justifie par l'impossibilité de garantir le niveau de sécurité d'un équipement personnel (absence de politique de sécurité appliquée, mises à jour non maîtrisées, risque de logiciels malveillants, absence de chiffrement des données). Un équipement personnel compromis pourrait servir de vecteur d'intrusion dans le réseau du client ou d'exfiltration de données confidentielles.

---

02. Équipements Mileo Technology autorisés

Mileo Technology met à disposition de ses techniciens l'ensemble des équipements nécessaires à leurs interventions : outillage électronique certifié (testeurs de câbles, analyseurs réseau, multimètres, testeurs d'image vidéo), tablettes professionnelles sous gestion MDM (Mobile Device Management) préconfigurées pour la documentation et la gestion des interventions, et postes de configuration dédiés pour le paramétrage des VMS, NVR et systèmes de contrôle d'accès.

Ces équipements sont inventoriés, tracés et font l'objet d'une politique de sécurité stricte : chiffrement complet du stockage, authentification forte, connexion VPN systématique pour les accès distants, et mises à jour de sécurité appliquées dans un délai de 72 heures après publication. Tout équipement Mileo Technology ne répondant plus à ces critères est retiré du parc et remplacé.

---

03. Interdiction d'utilisation des équipements informatiques clients

Il est formellement interdit à tout technicien Mileo Technology d'utiliser les équipements informatiques appartenant au client à des fins professionnelles, même avec l'autorisation verbale d'un interlocuteur du client. Cette règle s'applique aux postes de travail, serveurs, terminaux de configuration, connexions réseau filaires ou Wi-Fi, et à tout équipement connecté appartenant au client.

En cas de besoin d'accès à un équipement client dans le cadre de la configuration ou de la maintenance d'un système (par exemple, accès au VMS via le poste dédié du client), l'opération doit être réalisée sous la supervision directe du responsable informatique ou sécurité du client, qui conserve le contrôle de sa session. Le technicien peut guider la manipulation mais ne prend pas le contrôle de l'équipement.

---

04. Stockage des données sur supports chiffrés

Toutes les données collectées lors des interventions (photos, configurations, schémas, relevés techniques) doivent être stockées exclusivement sur les équipements Mileo Technology ou transférées vers la plateforme documentaire sécurisée de l'entreprise. L'utilisation de services de stockage en nuage personnels (Google Drive personnel,

Dropbox, WeTransfer) est interdite pour les données liées aux installations clients.

> **Les supports de stockage amovibles (clés USB, disques durs externes) utilisés pour le transfert de données entre équipements doivent être fournis par Mileo Technology et chiffrés (chiffrement AES-256 minimum). Tout support non chiffré est interdit sur les sites clients. En fin de mission, les données temporaires stockées sur les équipements de terrain doivent être transférées vers la plateforme centrale et supprimées de manière sécurisée des équipements locaux dans un délai de 48 heures.**

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