Politique BYOD techniciens

Référence	Version	Date	Catégorie
POL-CYB-007	v1.0	Mars 2025	Cybersécurité

L'utilisation d'équipements personnels (Bring Your Own Device) pour accéder aux systèmes de clients présente des risques de sécurité inacceptables dans le contexte de systèmes de sécurité physique. Mileo Technology interdit le BYOD pour tous les accès aux systèmes clients et fournit à ses techniciens les équipements nécessaires à l'exercice de leurs missions. Cette politique est une condition sine qua non de la confiance que nos clients nous accordent.

---

01. Interdiction du BYOD pour les accès clients

L'accès aux systèmes de vidéosurveillance, de contrôle d'accès et d'hypervision des clients est exclusivement réalisé depuis des équipements fournis et gérés par Mileo Technology. Sont concernés : les ordinateurs portables d'intervention, les tablettes de configuration, les smartphones professionnels.

Cette interdiction s'applique sans exception, y compris pour les accès distants réalisés depuis le domicile d'un technicien en astreinte. Un poste de travail professionnel ou une connexion VPN depuis un équipement professionnel est exigé. Aucune connexion depuis un équipement personnel ne peut être autorisée, même temporairement.

---

02. Exceptions documentées

Dans des circonstances exceptionnelles (équipement professionnel défaillant lors d'une urgence critique sans accès possible à un équipement de remplacement), une dérogation peut être accordée à titre ponctuel par le référent cybersécurité. Cette dérogation est limitée à la durée de l'urgence et documentée immédiatement.

Chaque exception est consignée dans le registre des dérogations : identité du technicien, date et durée, équipement personnel utilisé

(marque, modèle, système d'exploitation), justification, systèmes clients accédés. L'analyse de risque associée est réalisée et les mesures compensatoires appliquées sont documentées.

---

03. Cloisonnement des données

Les équipements professionnels de Mileo Technology sont configurés pour isoler les données professionnelles des usages personnels éventuels. Les données clients (configurations, captures d'écran, journaux d'intervention) ne peuvent être stockées que dans des espaces chiffrés dédiés, avec synchronisation vers les serveurs de Mileo Technology uniquement.

L'installation d'applications non approuvées sur les équipements professionnels est soumise à validation préalable. La liste des applications autorisées est maintenue par le responsable informatique. Les outils de synchronisation cloud personnels (Dropbox, OneDrive personnel, Google Drive personnel) sont bloqués.

---

04. Effacement à distance et chiffrement

Tous les équipements professionnels sont enrôlés dans la solution de gestion des appareils mobiles (MDM) de Mileo Technology. Cette solution permet l'effacement à distance de l'ensemble des données en cas de perte, de vol ou de départ d'un collaborateur.

> **Le chiffrement du stockage est activé sur l'ensemble des équipements professionnels : BitLocker sur Windows, FileVault sur macOS, chiffrement natif sur Android et iOS. La clé de chiffrement est séquestrée dans l'infrastructure de gestion centralisée, permettant une récupération par l'administrateur en cas de nécessité.**