Procédure d'accès distant sécurisé

Référence	Version	Date	Catégorie
PROC-CYB-001	v1.1	Avril 2025	Cybersécurité

> ***Prioritaire***

L'accès distant aux systèmes de sécurité de nos clients constitue un vecteur d'attaque privilégié qu'il convient de maîtriser rigoureusement. Cette procédure définit les conditions techniques et organisationnelles dans lesquelles Mileo Technology réalise des accès distants aux installations. Seuls les protocoles et outils approuvés sont autorisés ; tout accès non conforme est interdit et sanctionnable.

---

01. Protocoles autorisés

Les accès distants sont exclusivement réalisés via VPN IPSec ou VPN SSL/TLS avec authentification mutuelle par certificats. Le protocole SSH (version 2 uniquement) est autorisé pour l'administration des équipements Linux et des équipements réseau, avec authentification par clé publique obligatoire.

Le protocole RDP (Remote Desktop Protocol) en accès direct sur Internet est formellement interdit. Tout accès aux interfaces graphiques distantes doit transiter par le tunnel VPN préalablement établi. Les protocoles Telnet, FTP et HTTP (non chiffré) sont interdits pour tout usage d'administration.

Les accès via les interfaces cloud des constructeurs (P2P cloud) ne sont autorisés qu'à titre exceptionnel, sur accord préalable du référent cybersécurité, et uniquement pour des équipements dont le constructeur garantit le chiffrement de bout en bout. Un registre des exceptions est tenu à jour.

---

02. Processus d'autorisation préalable

Tout accès distant doit faire l'objet d'une autorisation préalable du client ou de son représentant désigné. Cette autorisation est tracée : email de confirmation, ticket d'intervention ouvert dans le système de gestion, ou validation via le portail client.

Pour les accès d'urgence en dehors des heures ouvrables, un contact d'astreinte client est identifié dans le contrat. L'accès sans autorisation préalable n'est possible qu'en cas d'urgence avérée, dûment documentée a posteriori dans un rapport d'intervention.

Les accès distants planifiés (maintenance préventive, mises à jour) sont programmés dans une fenêtre de maintenance convenue avec le client, avec un préavis minimum de 48 heures sauf urgence.

---

03. Durée et déconnexion automatique

La durée de chaque session d'accès distant est limitée à la durée strictement nécessaire à l'intervention. Le technicien se déconnecte immédiatement à l'issue de son intervention, sans laisser de session ouverte.

Les équipements VPN sont configurés avec un timeout d'inactivité de 15 minutes maximum. Toute session inactive au-delà de ce délai est automatiquement terminée. Les sessions VMS et interfaces web des NVR sont configurées avec un timeout de 10 minutes.

Aucun accès permanent n'est laissé ouvert sur les systèmes clients. Les comptes de maintenance créés pour une intervention sont désactivés ou supprimés immédiatement après l'intervention.

---

04. Traçabilité obligatoire

Chaque accès distant est documenté dans le système de ticketing de Mileo Technology : identité du technicien, date et heure de connexion et de déconnexion, objet de l'intervention, actions réalisées. Cette traçabilité est conservée 1 an minimum.

Les journaux de connexion VPN sont conservés par l'infrastructure Mileo Technology et peuvent être produits sur demande du client ou des autorités compétentes. Les équipements client (NVR, VMS)

génèrent leurs propres journaux d'accès, dont la conservation est vérifiée à chaque intervention.

Un rapport d'intervention est systématiquement produit et transmis au client dans les 24 heures suivant chaque accès distant. Ce rapport décrit les actions réalisées et les éventuelles anomalies constatées.

---

05. Équipements de connexion

Les accès distants sont réalisés exclusivement depuis des équipements fournis et gérés par Mileo Technology (ordinateurs portables d'entreprise). L'utilisation d'équipements personnels (BYOD) est formellement interdite pour tout accès aux systèmes clients.

> **Les postes de travail utilisés pour les accès distants font l'objet d'un durcissement spécifique : chiffrement du disque, antivirus à jour, pare-feu activé, accès restreint aux logiciels nécessaires. Ils sont soumis à une gestion centralisée (MDM) permettant leur contrôle et leur effacement à distance.**

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