# Procédure de révocation des accès

| Référence | Version | Date | Catégorie |
|---|---|---|---|
| **PROC-CYB-006** | v1.0 | Mars 2025 | Cybersécurité |

La révocation rapide des accès est un contrôle de sécurité critique souvent négligé. Un ancien collaborateur, un prestataire dont le contrat est terminé ou un compte compromis conservant des accès aux systèmes de vidéosurveillance représente une menace sérieuse et potentiellement indétectable. Mileo Technology impose une procédure de révocation rigoureuse avec des délais stricts selon la criticité des accès concernés.

---

## 01. Déclencheurs de révocation

La procédure de révocation est déclenchée dans les cas suivants : fin de contrat ou de prestation d'un collaborateur Mileo Technology ou d'un sous-traitant, changement de rôle d'un collaborateur entraînant la perte du besoin d'accès, suspicion ou confirmation de compromission d'un compte, signalement d'une utilisation frauduleuse ou anormale d'un accès.

Pour les accès aux systèmes clients, la révocation est également déclenchée sur demande du client (changement de prestataire, fin de la relation commerciale) et lors de la détection d'un compte inactif depuis plus de 90 jours (audit trimestriel des accès).

---

## 02. Délais de révocation

Les délais maximum de révocation sont définis selon la criticité de l'accès : accès distants actifs (VPN, comptes administrateurs VMS/NVR) — 2 heures maximum à compter du déclencheur ; comptes d'exploitation (opérateurs, visualisation) — 8 heures maximum ; accès physiques (badges, codes PIN) — 24 heures maximum.

En cas de suspicion de compromission ou d'incident de sécurité, le délai de révocation des accès critiques est ramené à 30 minutes. La révocation est prioritaire sur toute autre action de remédiation, afin de couper l'accès de l'attaquant potentiel avant de procéder à l'investigation.

---

## 03. Liste de contrôle des systèmes concernés

La révocation d'un accès doit couvrir l'ensemble des systèmes concernés. La check-list de révocation comprend : comptes VPN et certificats associés, comptes VMS et NVR sur tous les sites concernés, accès au gestionnaire de mots de passe, accès aux outils de collaboration et de gestion interne, comptes sur les portails constructeurs, clés SSH sur les équipements Linux.

Pour les collaborateurs de Mileo Technology, la check-list couvre également les accès aux systèmes internes : messagerie, outils de ticketing, accès à l'infrastructure d'hébergement. Le responsable RH et le référent cybersécurité coordonnent la révocation complète selon une liste de contrôle pré-établie.

---

## 04. Vérification post-révocation

Une vérification des accès est réalisée dans les 24 heures suivant la révocation pour s'assurer qu'aucun accès résiduel n'a été oublié. Cette vérification consiste à tenter une connexion avec les credentials révoqués (test de refus d'accès) et à analyser les journaux de connexion des 48 dernières heures pour détecter d'éventuelles connexions post-révocation.

> **En cas de détection d'une connexion réalisée après la révocation supposée, un incident de sécurité est immédiatement déclenché. Le résultat de la vérification post-révocation est documenté dans le ticket de révocation, qui est conservé 1 an.**