

# Gérer les accès et les départs de collaborateurs

Qui a accès à quoi ? Le principe du moindre privilège et la checklist départ qui évite les mauvaises surprises.

10 min de lecture · Niveau Intermédiaire · [cyberionis.fr/ressources/gestion-des-acces](https://cyberionis.fr/ressources/gestion-des-acces)

Les comptes dormants d'anciens collaborateurs et les droits accumulés au fil des années sont des portes dérobées involontaires. La gestion des accès est peu coûteuse, très efficace — et exigée par le RGPD.

## 1. Le principe du moindre privilège

Chacun ne doit accéder qu'à ce dont il a besoin pour son travail, rien de plus. Un commercial n'a pas besoin des dossiers RH ; un stagiaire n'a pas besoin d'être administrateur. Moins de droits, c'est moins de dégâts en cas de compte compromis — ou de maladresse.

- Comptes nominatifs uniquement : un compte partagé rend toute traçabilité impossible
- Droits administrateur réservés à l'administration, jamais pour l'usage quotidien
- Revue des accès une à deux fois par an : qui a encore accès à quoi, et pourquoi ?

## 2. L'arrivée d'un collaborateur

- Créer les comptes à partir d'une liste standard par poste
- Transmettre les mots de passe via le gestionnaire, jamais par email
- Faire signer la charte informatique dès le premier jour

## 3. Le départ : la checklist critique

- Désactiver tous les comptes le jour du départ (messagerie, VPN, logiciels métier, cloud)
- Changer les mots de passe des comptes partagés inévitables (réseaux sociaux, banque...)
- Récupérer matériel, badges et clés
- Retirer le collaborateur des accès tiers : prestataires, portails fournisseurs, listes de diffusion
- Transférer puis fermer la boîte email selon une règle définie à l'avance

## 4. Les accès qu'on oublie toujours

La messagerie et le VPN, tout le monde y pense. Voici ce qui passe systématiquement entre les mailles — et que les audits retrouvent des années après :

- Les réseaux sociaux de l'entreprise (LinkedIn, Instagram...) gérés depuis le compte personnel d'un salarié parti
- Le nom de domaine et l'hébergement du site, au nom de l'ancien « informaticien maison »

- Les prestataires externes qui ont encore un accès VPN ou TeamViewer « pour la maintenance »
- Les clés d'API et intégrations créées pour un projet et jamais révoquées
- Les box, imprimantes et caméras dont seul l'ancien collaborateur connaissait les mots de passe
- Les abonnements SaaS payés par carte, rattachés à l'email d'une personne et non de l'entreprise

#### ATTENTION

*Le risque du compte dormant n'est pas seulement l'ex-collaborateur malveillant (rare) : c'est surtout que personne ne surveille ce compte. Son mot de passe, souvent réutilisé, finit dans une fuite de données — et l'attaquant qui s'y connecte a tout son temps, puisque plus personne ne remarque rien sur un compte censé être inactif.*

---

## L'essentiel à retenir

- 01 Établir la cartographie « qui accède à quoi »
- 02 Supprimer les comptes génériques et les droits admin superflus
- 03 Rattacher domaine, hébergement et abonnements à l'entreprise, pas à une personne
- 04 Créer une checklist d'arrivée et de départ standardisée
- 05 Désactiver les comptes le jour même du départ
- 06 Inclure prestataires et intégrations dans la revue annuelle des accès

## Questions fréquentes

### Désactiver ou supprimer le compte d'un partant ?

Désactiver d'abord, supprimer plus tard : la désactivation immédiate coupe l'accès tout en préservant les emails et fichiers, le temps de les transférer et de respecter les durées de conservation. Fixez une règle (par exemple : désactivation le jour J, transfert sous 30 jours, suppression sous 6 mois) et appliquez-la uniformément — le RGPD n'aime pas les boîtes d'ex-salariés gardées indéfiniment.

### Comment gérer la boîte email d'un collaborateur parti ?

Réponse automatique indiquant le nouveau contact, transfert des messages professionnels vers le remplaçant pendant une durée limitée et annoncée, puis fermeture. La CNIL encadre ce point : le salarié doit être informé avant son départ, et la consultation de la boîte doit rester proportionnée — pas de lecture systématique des messages personnels.

### Un SSO (connexion unique), est-ce pour nous ?

Dès que vous jonglez avec plus d'une dizaine d'applications, oui : le SSO (via Microsoft Entra, Google Workspace...) centralise l'authentification — un seul compte à désactiver au départ coupe tous les accès d'un coup, et la MFA s'applique partout automatiquement. C'est l'outil qui transforme la checklist départ de 20 lignes en 3 lignes.

## Que faire face à un départ conflictuel ?

Anticiper : dans un contexte tendu, les accès se coupent au moment de l'annonce, pas à la fin du préavis — en coordination avec les RH et dans le respect du droit du travail. Vérifiez aussi les accès « souvenirs » : transferts automatiques vers une adresse personnelle, exports massifs de fichiers dans les semaines précédentes. Les journaux d'accès existent pour ça.

## Pour aller plus loin

CNIL — la vie du contrat de travail et les données — [www.cnil.fr/fr/travail-vie-privee](http://www.cnil.fr/fr/travail-vie-privee)

ANSSI — Guide d'hygiène informatique (gestion des comptes) — [cyber.gouv.fr/publications/guide-dhygiene-informatique](http://cyber.gouv.fr/publications/guide-dhygiene-informatique)

### Structurer sans vous noyer dans la paperasse ?

Audit, mise en conformité, chartes et sensibilisation des équipes : un accompagnement à la taille de votre entreprise.

[contact@cyberionis.fr](mailto:contact@cyberionis.fr) · 06 64 90 07 74 · [cyberionis.fr](http://cyberionis.fr)