# Checklist de récupération

Ce guide vous montre comment réagir de manière systématique en tant que PME en cas de perte de données - depuis les mesures immédiates jusqu'à la restauration.

## 1 - Mesures immédiates - garder son calme

- [ ] Informer le responsable informatique
- [ ] Déconnecter les appareils concernés du réseau
- [ ] Documenter les systèmes et les données affectés
- [ ] Ne pas effectuer de tentatives personnelles ni de restaurations sans l'accord du responsable informatique

## 2 - Analyse - compréhension de l'incident

- [ ] Vérification des données concernées (sauvegarde, données locales, services cloud)
- [ ] Identification de la cause (par ex. défaillance matérielle, ransomware, erreur humaine)
- [ ] Enregistrement des moments et des symptômes afin de déterminer l'ampleur
- [ ] Identifier les systèmes critiques pour le fonctionnement de l'entreprise

## 3 - Restauration - utiliser la sauvegarde

- [ ] Restaurer les données à partir de la dernière sauvegarde fonctionnelle
- [ ] Vérifier que la sauvegarde est complète et intacte
- [ ] Prioriser les systèmes critiques
- [ ] Tester les données et les systèmes après la restauration avant leur mise en service

## 4 - Communication - interne et externe

- [ ] Informer clairement les collaborateurs de l'incident et des étapes suivantes
- [ ] Si des clients sont concernés : informer de manière factuelle, sans créer de panique
- [ ] Tenir la direction régulièrement informée de l'évolution de la situation
- [ ] Utiliser des modèles de texte préparés (par ex. MOUNT10 KI-Prompt) pour une communication cohérente

# Checklist de récupération

Ce guide vous montre comment réagir de manière systématique en tant que PME en cas de perte de données - depuis les mesures immédiates jusqu'à la restauration.

### 5 - Mesures de sécurité - minimiser les risques futurs

| | |
|---|---|
| ☐ | Vérifier comment la perte de données s'est produite (faille de sécurité, absence d'isolation) |
| ☐ | Optimiser la stratégie de sauvegarde (sauvegardes régulières, sauvegarde immuable, systèmes séparés) |
| ☐ | Former régulièrement les collaborateurs dans le domaine de la sécurité des données |
| ☐ | Réaliser des tests de récupération réguliers |

### 6 - Le post-traitement - Lessons learned

| | |
|---|---|
| ☐ | Documenter l'incident (cause, durée, données concernées, mesures prises) |
| ☐ | Adapter les processus internes et les plans d'urgence |
| ☐ | Revue interne pour améliorer les responsabilités et les délais de réaction |
| ☐ | Mise à jour des listes de contrôle pour la sauvegarde et les urgences informatiques |

### En cas de vol de données

En cas de suspicion ou de confirmation d'un vol de données, **les autorités compétentes ou la police** doivent être informées. En Suisse, les obligations de notification s'appliquent conformément à la loi sur la protection des données (par ex. notification au Préposé fédéral à la protection des données et à la transparence – PFPDT en cas de violation de données).

### Recours à des spécialistes externes

En cas d'incidents de sécurité complexes, il peut être judicieux de faire appel à **une société externe spécialisée en réponse aux incidents et en criminalistique informatique**.
Les spécialistes externes peuvent apporter leur soutien pour : analyse des causes et préservation des preuves, évaluation des dommages, procédures conformes sur le plan juridique, restauration et durcissement des systèmes.