TROUSSE DE DÉMARRAGE CYBERSÉCURITÉ

Par où commencer

Le guide de la trousse : quels documents, dans quel ordre et pourquoi. Prévoyez quelques heures, réparties sur un mois.

Une PME n'a pas besoin d'un service de sécurité pour être bien préparée. Elle a besoin de **règles claires pour ses employés**, d'un **plan pour redémarrer**, d'une **marche à suivre quand ça arrive** et de **preuves à montrer à son assureur**. C'est exactement ce que contient cette trousse.

Les documents de la trousse

No	Document	Format	Rempli par
1	Politique d'utilisation des TI (à faire signer par chaque employé)	Word	Direction
2	Plan de reprise informatique	Word	Direction + TI
3	Plan de réponse aux incidents de cybersécurité	Word	Direction + TI
4	Formulaire de signalement d'incident	Word	Employés
5	Inventaire des actifs et fournisseurs	Excel	TI
6	Registre des incidents de confidentialité (Loi 25)	Excel	Responsable RP
7	Préparation à la cyberassurance	Excel	Direction + TI
8	Premiers gestes en cas de cyberattaque (affiche)	PDF	À imprimer
9	Contacts d'urgence	Word	Direction

Le plan en quatre semaines

Semaine 1 — Être prêt à réagir (1 heure)

- ☐ Remplir la fiche **9 – Contacts d'urgence** et en garder une copie hors du bureau.
- ☐ Imprimer et afficher **8 – Premiers gestes** près des postes de travail.
- ☐ Désigner le responsable de la protection des renseignements personnels et ouvrir le **6 – Registre Loi 25**.

Semaine 2 — Encadrer les employés (1 à 2 heures)

- ☐ Adapter la **1 – Politique d'utilisation**, la présenter à l'équipe et la faire signer.
- ☐ Distribuer le **4 – Formulaire de signalement** et expliquer qu'on ne blâme pas celui qui signale.

Semaine 3 — Connaître ce qu'on protège (2 heures, avec votre TI)

- ☐ Remplir le **5 – Inventaire** : appareils, logiciels, fournisseurs, comptes administrateurs.
- ☐ Compléter le **2 – Plan de reprise** : priorités, délais acceptables, sauvegardes.

Semaine 4 — Se préparer au pire et à l'assureur (2 heures)

- ☐ Adapter le **3 – Plan de réponse** et faire un exercice de 30 minutes : « un employé appelle, ses fichiers sont chiffrés ».
- ☐ Remplir le **7 – Préparation à la cyberassurance** et corriger d'abord les contrôles critiques manquants.

Les cinq protections que tout assureur vérifie

- **Double authentification (MFA)** sur le courriel, les accès à distance et les comptes administrateurs.
- **EDR** (antivirus nouvelle génération avec détection et réponse) sur tous les postes et serveurs.
- **Sauvegardes immuables ou hors ligne**, testées au moins une fois par année.
- **Procédure de paiement** : tout changement bancaire est confirmé par téléphone.
- **Formation des employés**, au moins une fois par année.

S'il en manque une seule, la prime augmente, une exclusion s'applique… ou la réclamation peut être refusée.

Pour aller plus loin

Articles du blog **supportadistance.com/blog-et-nouveautes** :

- 12 étapes pour protéger votre entreprise : /12-etapes-proteger-entreprise-2026/
- La fraude du président : /fraude-du-president/
- La fraude à la paie : /fraude-a-la-paie/
- Compte piraté, 5 étapes : /compte-pirate-5-etapes/
- Clés d'accès (passkeys) : /cles-d-acces-passkeys/

> **Besoin d'aide pour remplir la trousse ?**
>
> Appelez le tech peut évaluer votre environnement, remplir l'inventaire et la liste de contrôle de l'assureur avec vous, et mettre en place les protections manquantes.
>
> **514-444-1041** · supportadistance.com/contact

Ces documents sont des modèles à adapter. Ils ne constituent pas un avis juridique ; validez les obligations légales et contractuelles avec votre conseiller juridique ou votre courtier.