cyberdiagnostic

ÉVALUEZ. COMPRENEZ. PROTÉGEZ.
VOTRE CYBERSÉCURITÉ EN 10 MINUTES.

# KIT PME — CYBERSÉCURITÉ & CONFORMITÉ

## Les documents essentiels du dirigeant de PME de 5 à 50 salariés

Édition 2026 · Alignée sur les recommandations de l'ANSSI, de la CNIL et sur les exigences de sécurité de la chaîne d'approvisionnement (NIS2)

**Évaluez. Comprenez. Protégez.**

Votre cybersécurité en 10 minutes · cyberdiagnostic.fr

DOCUMENT 00

# Guide d'utilisation du kit

Par où commencer, qui fait quoi, et les 10 mesures qui comptent vraiment.

Une PME n'a ni RSSI ni service juridique dédié. Ce kit vous donne **cinq modèles prêts à remplir** et une fiche réflexe, construits pour être appliqués en quelques heures, pas en quelques mois. Les champs en vert sont **modifiables directement dans le PDF** (Acrobat Reader, Aperçu, navigateur), puis imprimables ou signables.

## Mode d'emploi en 3 étapes

| Étape | Action | Durée indicative |
|---|---|---|
| **1 · Désigner** | Nommez un référent cybersécurité (vous, un associé ou un prestataire) et une personne de remplacement. Il pilote le kit. | 15 min |
| **2 · Remplir** | Complétez les documents dans l'ordre conseillé ci-dessous. Adaptez, supprimez ce qui ne vous concerne pas : mieux vaut un document court et vrai qu'un document complet et ignoré. | 1 à 2 h par document |
| **3 · Diffuser et tester** | Faites signer la charte, planifiez le premier test de restauration, imprimez la fiche réflexe. Révisez le tout une fois par an. | 1 h + 1 h/trimestre |

## Les documents du kit

| N° | Document | À quoi il sert | Priorité |
|---|---|---|---|
| 01 | Charte informatique | Fixe les règles d'usage des outils numériques et protège l'entreprise comme les salariés. | Haute |
| 02 | Plan de sauvegarde & reprise | Garantit que vous pouvez repartir après une panne, un vol ou un rançongiciel. | Très haute |
| 03 | Registre RGPD | Obligation légale (art. 30) : recense vos traitements, sous-traitants et violations. | Haute |
| 04 | Questionnaire fournisseur | Répondre vite et juste aux questionnaires sécurité de vos clients et donneurs d'ordres. | Moyenne |
| 05 | Fiche réflexe incident | Les 60 premières minutes : qui appeler, quoi faire, quoi ne pas faire. | Très haute |

**Ordre conseillé**
05 Fiche réflexe, puis 02 Sauvegarde, 01 Charte, 03 Registre RGPD et enfin 04 Questionnaire fournisseur. Commencez par ce qui limite les dégâts, puis ce qui prévient, puis ce qui prouve.



*Modèle fourni à titre informatif, à adapter à votre situation. Il ne constitue pas un avis juridique.*

# Les 10 mesures prioritaires de votre PME

Cochez ce qui est en place aujourd'hui. Chaque case non cochée est une piste d'action concrète. Pour un niveau de maturité chiffré et un plan d'action priorisé, le diagnostic en ligne **cyberdiagnostic.fr** évalue votre entreprise en 10 minutes.

- ☐ **Authentification multifacteur** activée sur la messagerie, les accès à distance et les comptes administrateurs.
- ☐ **Mots de passe robustes** (12 caractères minimum ou phrase de passe), uniques, gérés dans un coffre-fort de mots de passe.
- ☐ **Mises à jour** automatiques des postes, serveurs, box/pare-feu et logiciels métier (correctifs critiques sous 15 jours).
- ☐ **Sauvegardes 3-2-1** dont une copie déconnectée ou immuable, avec un test de restauration réussi dans les 3 derniers mois.
- ☐ **Antivirus / EDR** sur tous les postes et serveurs, supervisé, avec chiffrement des disques des ordinateurs portables.
- ☐ **Comptes nominatifs** et droits au strict nécessaire ; comptes administrateurs distincts des comptes du quotidien.
- ☐ **Sensibilisation** des équipes au phishing au moins une fois par an (et à chaque arrivée de nouveau salarié).
- ☐ **Charte informatique** signée par tous les salariés et procédure d'arrivée/départ (création et suppression des accès).
- ☐ **Registre RGPD** à jour, liste des sous-traitants et contrats de sous-traitance (art. 28) signés.
- ☐ **Plan de réponse à incident** imprimé : contacts d'urgence, réflexes, notification CNIL sous 72 h si données personnelles, déclaration à l'assureur.

> **Le point de vue de l'expert**
> Les attaques visant les PME exploitent presque toujours les mêmes failles : un compte sans double authentification, un correctif non appliqué, une sauvegarde inaccessible ou jamais testée, un salarié non sensibilisé. Ces dix mesures couvrent l'essentiel du risque réel pour un coût maîtrisé.

## Comment ce kit s'inscrit dans le cadre réglementaire

- **RGPD** : registre des traitements (art. 30), sécurité du traitement (art. 32), notification des violations sous 72 h (art. 33), sous-traitants (art. 28).
- **NIS2** : même si votre entreprise n'est pas directement concernée, vos clients concernés doivent maîtriser leur chaîne d'approvisionnement et vous poseront des questions de sécurité (document 04).
- **Recommandations ANSSI / Cybermalveillance.gouv.fr** : hygiène informatique, sauvegarde, gestion des incidents.

Ces modèles sont des supports pratiques de bonne pratique. Ils doivent être adaptés à la taille, à l'activité et au contexte de votre entreprise ; en cas de doute juridique (droit du travail, contrats), faites-les valider par votre conseil.



*Modèle fourni à titre informatif, à adapter à votre situation. Il ne constitue pas un avis juridique.*