

# La charte cyber du responsable d'entreprise

12 engagements et 7 piliers pour protéger son entreprise

Un document écrit pour les dirigeants de très petites et moyennes entreprises, et non pour les informaticiens. Il ne demande aucun budget pour être lu, aucune compétence technique pour être compris, et son premier engagement ne coûte rien d'autre qu'un peu d'honnêteté.

|             |                                                                              |
|-------------|------------------------------------------------------------------------------|
| Référence   | MCC-CHARTe-DIR-001                                                           |
| Version     | 1.0 — 28 août 2026                                                           |
| Public visé | Dirigeants de TPE, PME et ETI, artisans, professions libérales, associations |
| Diffusion   | Libre — reproduction encouragée sous réserve de mention de la source         |

## POURQUOI CETTE CHARTE

## Personne ne vous a jamais parlé du risque cyber comme d'une habitude

On vous a vendu des logiciels. On vous a parlé de pare-feu, d'antivirus, de sauvegarde dans le nuage. On vous a peut-être fait un devis. Ce qu'on ne vous a probablement jamais dit, c'est que **le principal obstacle n'est pas technique : il est humain**, et qu'il ressemble beaucoup à ce que traverse quelqu'un qui affronte une dépendance.

Cette charte emprunte donc sa forme au cheminement en douze étapes des mouvements d'entraide en alcoologie. Ce n'est ni une plaisanterie ni une provocation : c'est un hommage à une méthode qui fonctionne depuis près d'un siècle, parce qu'elle a compris quelque chose que les catalogues de solutions ignorent. On ne change pas durablement par un achat. On change par la lucidité, la régularité, l'humilité, l'entourage et la transmission.

Regardez si ces phrases vous sont familières.

**LES SIX ÉTAPES QUE TRAVERSE PRESQUE TOUT DIRIGEANT**

- **Le déni** — « nous sommes trop petits, nous n'intéressons personne ».
- **La minimisation** — « on a un antivirus, c'est déjà pas mal ».
- **La délégation magique** — « c'est le problème de l'informatique, pas le mien ».
- **La honte** — « si ça nous arrive, surtout que ça ne se sache pas ».
- **La rechute** — six mois après l'alerte, tout le monde est retourné à ses habitudes.
- **L'acceptation** — le risque ne disparaîtra jamais. Il se gère. Un jour après l'autre.

Si vous en reconnaissez au moins deux, cette charte est faite pour vous.

## CE QUI EST EN JEU

## Sept protections, et pas une de plus

Cette charte n'a pas pour objet la conformité, ni le zéro risque, ni la performance technique. Elle a un objet unique : que votre entreprise soit encore là dans cinq ans, avec ses clients et ses salariés.

| PROTECTION                | CE QUI EST RÉELLEMENT EN JEU                                                                                             |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------|
| L'entreprise              | La capacité à ouvrir et à travailler demain matin.                                                                       |
| Le chiffre d'affaires     | Les jours d'arrêt facturés à zéro, les commandes perdues, la trésorerie qui se vide pendant que les salaires continuent. |
| L'image                   | Une confiance qui met dix ans à se construire et deux heures à s'effondrer.                                              |
| Les emplois               | Le chômage technique, puis les départs, puis parfois la cessation de paiement.                                           |
| Le service aux clients    | Les livraisons, les délais, les engagements tenus. Et le client qui, lui, ne peut pas attendre.                          |
| Les échanges fournisseurs | La facturation, les virements détournés, la confiance de toute la filière.                                               |
| Les données               | Le fichier clients, les prix, le savoir-faire, et les données personnelles dont vous répondez devant la CNIL.            |

## PREMIÈRE PARTIE

# Les 12 engagements du dirigeant

Ils se lisent dans l'ordre. Chacun rend le suivant possible. Vous n'êtes pas obligé de tous les tenir cette année : vous êtes seulement obligé de commencer par le premier.

## ENGAGEMENT 01

## Je reconnais que mon entreprise est une cible

**L'esprit.** Tout commence par la fin du déni. Les attaques ne vous choisissent pas : elles sont automatisées, elles ratissent, elles ramassent ce qui est mal fermé. Être petit ne protège pas — cela rend seulement plus facile.

**JE M'ENGAGE À**

reconnaître que la question n'est pas « si » mais « quand », et que je ne dispose pas seul de toutes les compétences pour y répondre.

**Concrètement cette semaine :** j'écris en une page ce qui se passe si lundi matin plus aucun ordinateur ne démarre. Je chiffre le coût d'une journée d'arrêt total — chiffre d'affaires perdu, salaires versés à vide, pénalités, clients partis. Et je dis ce chiffre à voix haute devant mon équipe.

## ENGAGEMENT 02

## J'admets qu'une réponse existe et qu'elle est à ma portée

**L'esprit.** Après le déni vient le découragement : « c'est trop complexe, trop cher, c'est bon pour les grands groupes ». C'est faux. L'immense majorité des attaques qui réussissent chez les petites structures exploitent des failles élémentaires : un mot de passe faible, une mise à jour jamais faite, une sauvegarde qui n'existe pas, un salarié que personne n'a prévenu.

**JE M'ENGAGE À**

ne plus me réfugier derrière la complexité pour ne rien faire.

**Concrètement cette semaine :** je lis le guide de l'ANSSI destiné aux TPE et PME, et je repère les trois mesures qui, chez moi, offrent le meilleur rapport protection sur coût.

## ENGAGEMENT 03

## Je décide que ce sujet est le mien, pas celui de l'informatique

**L'esprit.** C'est l'étape de la décision, et la plus déterminante. Tant que le sujet reste technique, il reste orphelin. La cybersécurité n'est pas une question d'informatique : c'est une question de trésorerie, de continuité, d'emploi et de réputation. Elle vous appartient donc, exactement comme la sécurité au travail.

**JE M'ENGAGE À**

porter personnellement ce risque. Je peux en déléguer l'exécution ; je ne délègue jamais la responsabilité.

**Concrètement ce mois-ci :** j'inscris un point cyber récurrent — quinze minutes suffisent — à mes réunions de direction. Je nomme un référent interne, même à temps très partiel, avec un mandat écrit. J'ouvre une ligne budgétaire identifiée, si modeste soit-elle, et je la maintiens même les années sans incident.

## ENGAGEMENT 04

## Je fais un inventaire honnête, sans me raconter d'histoires

**L'esprit.** On ne protège que ce que l'on connaît. Cet inventaire doit accepter de faire mal : le serveur de sauvegarde débranché depuis huit mois, le compte du prestataire parti il y a trois ans et toujours actif, le mot de passe de la comptabilité collé sous le clavier.

**JE M'ENGAGE À**

dresser un état des lieux sincère de mes équipements, de mes applications, de mes données vitales, de mes accès et de mes dépendances — sans en minimiser les faiblesses.

**Concrètement ce mois-ci :** je liste les postes, serveurs, téléphones, machines de production et objets connectés, y compris ceux qu'on ne touche plus. Je liste les logiciels et services en ligne, y compris ceux souscrits par un service sans passer par personne. Et je réponds à une seule question : *sans quel fichier mon entreprise s'arrête-t-elle ?*

## ENGAGEMENT 05

## Je montre cet état des lieux à quelqu'un d'autre

**L'esprit.** Un inventaire qui reste dans un tiroir ne sert à rien. Le dire à voix haute à quelqu'un transforme un constat en engagement. C'est aussi le moment où l'on découvre que les autres dirigeants vivent exactement la même chose, et que la honte n'a aucune raison d'être.

**JE M'ENGAGE À**

présenter mon état des lieux à au moins une personne extérieure compétente, et à accepter son regard sans me justifier.

**Concrètement :** je demande un diagnostic gratuit et sans vente via MonAideCyber, ou je sollicite une association d'accompagnement. J'en profite pour relire ce que couvre — et surtout ce que ne couvre pas — le contrat de mon prestataire informatique.

## ENGAGEMENT 06

## Je me déclare prêt à renoncer aux facilités dangereuses

**L'esprit.** Toute dépendance repose sur des habitudes confortables. En cybersécurité, elles ont un nom : le mot de passe unique partagé par toute l'équipe, le compte administrateur utilisé pour le courriel du matin, la clé USB qui circule, le logiciel « qu'on ne peut pas mettre à jour parce que ça marche », l'accès à distance ouvert à tous vents. Renoncer est inconfortable — c'est précisément pour cela que c'est une étape.

**JE M'ENGAGE À**

abandonner ces commodités, y compris quand elles me font gagner du temps, y compris quand elles sont les miennes.

**Concrètement :** je commence par moi. Le dirigeant est la cible numéro un et, très souvent, le premier à réclamer une exception. Une mesure qui gêne un peu tout le monde vaut toujours mieux qu'un arrêt qui bloque tout le monde.

## ENGAGEMENT 07

## Je demande de l'aide, avec humilité

**L'esprit.** Un patron est censé tout savoir. En cybersécurité, faire semblant de savoir est le plus court chemin vers l'incident. Demander de l'aide n'est pas un aveu de faiblesse : c'est la seule stratégie rationnelle face à un adversaire organisé, financé et professionnel.

**JE M'ENGAGE À**

m'entourer avant la crise, et non pendant.

**Concrètement ce mois-ci :** j'établis la liste de qui appeler — prestataire, assureur, Cybermalveillance.gouv.fr, 17Cyber, gendarmerie ou police. Je l'imprime sur papier : le jour où j'en aurai besoin, mon système d'information sera peut-être hors service.

## ENGAGEMENT 08

## J'établis la liste de tous ceux qui paieraient

**L'esprit.** Le risque cyber n'est jamais un risque personnel : il se propage. Une attaque n'atteint pas seulement le dirigeant. Elle atteint les salariés au chômage technique, les clients livrés en retard, les fournisseurs non payés, les partenaires contaminés par rebond, et les familles derrière chacun d'eux.

**JE M'ENGAGE À**

nommer ces personnes, et à considérer leur protection comme partie intégrante de mon métier de dirigeant.

**Concrètement :** j'écris la liste — salariés, clients, fournisseurs, sous-traitants, banque, assureur, associés — et en face de chacun, en une ligne, ce qu'il perdrait. Je relis cette page au moment d'arbitrer un budget.

## ENGAGEMENT 09

## Je répare, en commençant par ce qui protège le plus

**L'esprit.** C'est l'étape de l'action. Elle doit être priorisée, pas exhaustive : trois mesures réellement appliquées valent mieux que trente inscrites dans un plan que personne n'exécutera. On commence par ce qui empêche l'entreprise de mourir.

**JE M'ENGAGE À**

tenir un plan d'actions priorisé, daté et suivi, et à préférer l'exécution à la planification.

**Le socle vital, dans cet ordre :**

- **Les sauvegardes** — trois copies, deux supports, une hors ligne et hors site. Et surtout : **une restauration réellement testée**. Une sauvegarde jamais restaurée n'est pas une sauvegarde, c'est une croyance.
- **La double authentification** sur la messagerie, la banque et les accès à distance. La meilleure mesure qui existe au rapport efficacité sur prix.
- **Les mises à jour**, en priorité sur tout ce qui est exposé sur Internet.
- **La séparation des comptes** : plus personne ne travaille au quotidien avec un compte administrateur.
- **La double validation des virements et des changements de RIB**, par un autre canal que celui de la demande. Cette seule mesure arrête l'essentiel de la fraude au président et de la fausse facture.

## ENGAGEMENT 10

## Je continue l'inventaire, et quand j'ai tort je le dis vite

**L'esprit.** L'inventaire n'est pas un événement, c'est une pratique. Les prestataires changent, les salariés arrivent et partent, les usages dérivent. Une photo prise il y a deux ans ne décrit plus rien. Et quand une erreur est commise — un clic malheureux, une consigne oubliée — la reconnaître dans l'heure est ce qui sépare l'incident maîtrisé de la catastrophe.

**JE M'ENGAGE À**

réviser régulièrement mon état des lieux et à faire en sorte que, chez moi, signaler une erreur soit valorisé et jamais sanctionné.

**Concrètement :** je supprime les accès des partants le jour de leur départ, sans exception ni délai. J'affiche une règle simple : *celui qui signale un doute a toujours bien fait, même si c'était une fausse alerte*. Et je tiens un petit journal des incidents, même mineurs : les petits signaux annoncent les grands.

## ENGAGEMENT 11

## Je cultive la vigilance collective et je m'entraîne à froid

**L'esprit.** La sécurité ne tient pas dans les outils, elle tient dans les gens. Une équipe entraînée repère ce qu'aucun logiciel ne voit. Et une crise se gère infiniment mieux quand on l'a répétée : découvrir le jour J que personne ne sait qui décide, qui parle aux clients et où sont les sauvegardes coûte des semaines.

**JE M'ENGAGE À**

sensibiliser mes équipes en continu et à préparer mon entreprise à tourner en mode dégradé.

**Concrètement cette année :** une sensibilisation courte deux fois par an et à chaque embauche ; une fiche réflexe d'une page affichée ; un plan de continuité minimal — comment je prends les commandes, je livre et je facture pendant une semaine sans informatique ; un exercice de crise, même informel, une heure autour d'une table.

## ENGAGEMENT 12

## Ayant progressé, je transmets et j'aide mes pairs

**L'esprit.** C'est l'aboutissement, et c'est la clé de voûte. Une filière économique est un écosystème : le fournisseur compromis devient mon problème, le client compromis devient mon risque. Personne n'est protégé seul. Partager son expérience, y compris ses incidents, est un acte de solidarité économique — et le meilleur moyen d'ancrer ses propres pratiques.

**JE M'ENGAGE À**

rompre le silence qui entoure les attaques et à élever le niveau de ceux qui travaillent avec moi.

**Concrètement :** je parle de mes incidents, même anonymisés, dans mon réseau professionnel. J'interroge mes fournisseurs critiques sur leurs pratiques et j'inscris quelques exigences simples dans mes contrats. J'accompagne un confrère plus petit. Et je dépose plainte systématiquement : le silence ne protège que l'agresseur.

## DEUXIÈME PARTIE

## Les 7 piliers de la sagesse cyber

Les douze engagements décrivent un chemin. Les sept piliers décrivent l'état d'esprit qui permet de le tenir dans la durée — c'est-à-dire au-delà du sixième mois, quand l'émotion de l'alerte est retombée.

## PILIER 1

### La lucidité

« *On ne guérit pas de ce qu'on refuse de voir.* »

Le déni est le premier ennemi, très loin devant le pirate. Il ne s'agit pas de vivre dans la peur, mais de préférer une mauvaise nouvelle vraie à une bonne nouvelle fausse.

**En pratique** : je mesure au lieu de supposer. Je teste mes sauvegardes au lieu de croire qu'elles fonctionnent.

## PILIER 2

### La sobriété

« *Ce qui n'existe pas ne peut pas être attaqué.* »

La sécurité progresse d'abord par soustraction. Chaque compte inutile, chaque logiciel oublié, chaque accès distant laissé ouvert, chaque donnée conservée sans raison est une porte de plus.

**En pratique** : je ferme, je supprime, je désinstalle, je restreins — avant d'acheter quoi que ce soit.

## PILIER 3

### La régularité

« *La constance vaut mieux que l'exploit.* »

Un audit brillant suivi de deux ans d'inaction protège moins qu'une routine modeste tenue chaque mois. La sécurité est une hygiène, pas un projet. Elle se pratique un jour après l'autre, avec des gestes petits, répétés, ennuyeux — et c'est parce qu'ils sont ennuyeux qu'ils fonctionnent.

**En pratique** : un rendez-vous cyber récurrent dans l'agenda, tenu même — surtout — quand tout va bien.

## PILIER 4

### La transparence

« *Le silence est l'allié de l'attaquant.* »

Un salarié qui n'ose pas dire qu'il a cliqué fait perdre la demi-journée qui comptait. Une entreprise qui cache son attaque prive toute sa filière d'un signal d'alerte. La transparence est une mesure de sécurité à part entière.

**En pratique** : on ne sanctionne jamais celui qui signale. On le remercie.

**PILIER 5****L'entourage**

*« Personne ne s'en sort seul. »*

Le dirigeant isolé face au risque cyber décide systématiquement trop tard, trop cher, ou au mauvais endroit. L'entourage, ce sont les pairs, les réseaux de dirigeants, les prestataires, les organismes publics. C'est aussi, en interne, l'équipe à qui l'on donne le droit de contredire le patron.

**En pratique** : je connais avant la crise les trois personnes que j'appellerai pendant la crise.

**PILIER 6****La préparation à la rechute**

*« L'incident arrivera. La seule question est de savoir dans quel état il nous trouvera. »*

Aucune protection n'est totale. Considérer l'incident comme une possibilité normale, et non comme un échec honteux, change tout : on prépare, on répète, on prévoit le mode dégradé. Ceux qui se relèvent vite ne sont pas ceux qui n'ont jamais été touchés ; ce sont ceux qui avaient prévu de l'être.

**En pratique** : je sais faire tourner mon entreprise une semaine sans informatique — et je l'ai vérifié.

**PILIER 7****La transmission**

*« Ce que l'on garde pour soi s'affaiblit ; ce que l'on partage s'enracine. »*

Expliquer à un confrère pourquoi on rappelle toujours avant de changer un RIB ancre la pratique bien mieux qu'une procédure écrite. Dans une économie où chacun est le maillon d'une chaîne, élever le niveau de son voisin, c'est élever le sien.

**En pratique** : je parle de cybersécurité à au moins un autre dirigeant chaque trimestre.

## TROISIÈME PARTIE

## Par quoi je commence, et quand

Une charte que l'on approuve sans rien changer ne protège personne. Voici la traduction des douze engagements en trois échéances tenables, même sans service informatique.

### Dans les 30 jours – arrêter l'hémorragie possible

- Vérifier qu'une sauvegarde existe hors ligne, et **en tester une restauration réelle**.
- Activer la double authentification sur la messagerie, la banque et les accès à distance.
- Instaurer la double validation des virements et des changements de coordonnées bancaires.
- Imprimer la liste des numéros à appeler en cas d'incident et l'afficher.
- Chiffrer le coût d'une journée d'arrêt et l'annoncer en réunion.

### Dans les 90 jours – poser le socle

- Terminer l'inventaire des équipements, logiciels, données et accès.
- Supprimer les comptes inutiles et les accès des personnes parties.
- Mettre à jour en priorité tout ce qui est exposé sur Internet.
- Séparer les comptes administrateurs des comptes de travail quotidien.
- Sensibiliser tout le monde et diffuser la fiche réflexe.
- Écrire le plan de continuité minimal.

### Dans les 12 mois – installer la durée

- Tenir le point cyber récurrent en réunion de direction.
- Réaliser un exercice de crise, même court.
- Interroger les prestataires et fournisseurs critiques.
- Revoir l'inventaire et le plan d'actions.
- Partager son expérience avec au moins trois autres dirigeants.

| INDICATEUR                                             | CIBLE                     |
|--------------------------------------------------------|---------------------------|
| Dernière restauration de sauvegarde testée avec succès | <b>moins de 3 mois</b>    |
| Accès critiques protégés par double authentification   | <b>100 %</b>              |
| Délai de suppression des accès d'un partant            | <b>moins de 24 heures</b> |
| Collaborateurs sensibilisés dans l'année               | <b>100 %</b>              |
| Doutes signalés par les collaborateurs                 | <b>en hausse</b>          |
| Dernier exercice de crise                              | <b>moins de 12 mois</b>   |
| Point cyber tenu en réunion de direction               | <b>à chaque séance</b>    |

#### À LIRE DANS LE BON SENS

**Un nombre de signalements en hausse est un bon signe**, pas un mauvais : il traduit une équipe qui ose parler. C'est le silence qu'il faut craindre.

## S'ENGAGER

## Engagement du dirigeant

Je soussigné(e) .....

agissant en qualité de .....

de l'entreprise .....

Je reconnais que la sécurité numérique de mon entreprise relève de ma responsabilité personnelle de dirigeant.

Je m'engage à mettre en œuvre les douze engagements de cette charte selon une feuille de route que je fixe et que je suis, et à faire vivre les sept piliers dans les pratiques quotidiennes de mon entreprise.

Je déclare agir ainsi pour protéger l'activité de mon entreprise, son chiffre d'affaires, son image, les emplois de mes collaborateurs, le service rendu à mes clients, la relation avec mes fournisseurs et les données qui m'ont été confiées.

Fait à ....., le ..... / ..... / .....

Signature :

## Contacts et ressources utiles

- **Cybermalveillance.gouv.fr** — assistance aux victimes, diagnostic, annuaire de prestataires labellisés.
- **MonAideCyber** (monaide.cyber.gouv.fr) — diagnostic gratuit accompagné par un aidant référencé par l'ANSSI.
- **17Cyber** — signalement et orientation en cas d'attaque.
- **ANSSI** (cyber.gouv.fr) — guides d'hygiène informatique pour les TPE et PME.
- **CNIL** — obligations relatives aux données personnelles et notification des violations.
- **MON COPAIN CYBER** — Contact@moncopaincyber.fr — www.moncopaincyber.fr — accompagnement gratuit, sans condition et sans contrepartie.

*Document élaboré par l'association MON COPAIN CYBER. Sa structure s'inspire, avec respect, du cheminement en douze étapes des mouvements d'entraide en alcoologie ; aucun lien, affiliation ou approbation de leur part n'est suggéré. Cette charte est un engagement volontaire : elle ne constitue ni un référentiel normatif, ni un avis juridique. Diffusion libre, reproduction encouragée sous réserve de mention de la source.*