CHECKLIST CYBERSÉCURITÉ PME

20 MESURES ESSENTIELLES

AUTO-ÉVALUATION

Cochez chaque mesure déjà en place dans votre organisation — Total sur 20

🔐 MOTS DE PASSE & ACCÈS

- ☐ 01 **Gestionnaire de mots de passe déployé** — CRITIQUE
  Bitwarden, 1Password, KeePass… pour tous les collaborateurs
- ☐ 02 **Double authentification (2FA) activée** — CRITIQUE
  Sur messagerie, VPN, outils cloud, accès distants
- ☐ 03 **Politique de mots de passe formalisée** — IMPORTANT
  Longueur minimale 12 car., complexité, renouvellement
- ☐ 04 **Principe du moindre privilège appliqué** — IMPORTANT
  Chaque utilisateur accède uniquement à ce dont il a besoin
- ☐ 05 **Comptes administrateurs distincts des comptes courants** — IMPORTANT
  Un admin ne navigue pas sur Internet avec son compte admin

📡 RÉSEAU & EMAILS

- ☐ 11 **Pare-feu configuré et maintenu** — CRITIQUE
  Règles à jour, logs activés, revue périodique
- ☐ 12 **Filtrage des emails (anti-spam / anti-phishing)** — CRITIQUE
  Solution dédiée ou option activée chez l'hébergeur mail
- ☐ 13 **SPF, DKIM et DMARC configurés** — IMPORTANT
  Protection contre l'usurpation de votre domaine email
- ☐ 14 **VPN pour les accès distants** — IMPORTANT
  Télétravail, déplacement — jamais de connexion directe RDP
- ☐ 15 **Wi-Fi invité séparé du réseau interne** — UTILE
  VLAN distinct, accès internet uniquement pour les visiteurs

💾 SAUVEGARDES & MISES À JOUR

- ☐ 06 **Sauvegardes régulières selon règle 3-2-1** — CRITIQUE
  3 copies, 2 supports différents, 1 hors site / hors ligne
- ☐ 07 **Tests de restauration effectués** — CRITIQUE
  Une sauvegarde non testée n'est pas une sauvegarde fiable
- ☐ 08 **Mises à jour OS et logiciels automatisées** — CRITIQUE
  Patchs de sécurité appliqués dans les 30 jours suivant la sortie
- ☐ 09 **Antivirus / EDR déployé sur tous les postes** — IMPORTANT
  Solution managée, alertes centralisées, signatures à jour
- ☐ 10 **Inventaire matériel et logiciel tenu à jour** — UTILE
  Vous ne pouvez pas protéger ce que vous ne connaissez pas

👥 SENSIBILISATION & PROCÉDURES

- ☐ 16 **Formation cybersécurité des collaborateurs** — CRITIQUE
  Au minimum une fois par an, avec exercice de phishing simulé
- ☐ 17 **Procédure de gestion des incidents formalisée** — CRITIQUE
  Qui appeler ? Quoi faire ? Contacts d'urgence affichés
- ☐ 18 **Procédure de départ salarié documentée** — IMPORTANT
  Révocation des accès le jour J, récupération du matériel
- ☐ 19 **Charte informatique signée par tous** — IMPORTANT
  Usages acceptables, responsabilités, règles BYOD
- ☐ 20 **Assurance cyber souscrite** — UTILE
  Couverture incidents, assistance en cas d'attaque

0 – 9	10 – 14	15 – 18	19 – 20
Niveau critique — Risque maximal. Agir immédiatement.	Niveau insuffisant — Des failles importantes persistent.	Niveau satisfaisant — Quelques axes d'amélioration.	Niveau excellent — Maintenez et testez régulièrement.

Besoin d'un audit de sécurité ou d'un plan d'action priorisé pour votre PME ?

ayinedjimi-consultants.fr/contact