



## CHARTRE DE SÉCURITÉ INFORMATIQUE



Gbessia Kondebougni, Matoto



+224 620 451 485



cabinet.pem@gmail.com



www.pemsarl.com

**Charte de Sécurité Informatique** \_\_\_\_\_ **3**

**Objectifs de la Charte :** \_\_\_\_\_ **3**

1. Renforcer la cybersécurité : \_\_\_\_\_ **3**

2. Maintenir l' intégrité des données : \_\_\_\_\_ **3**

3. Garantir la disponibilité des systèmes : \_\_\_\_\_ **3**

4. Respecter les réglementations : \_\_\_\_\_ **3**

5. Former et sensibiliser : \_\_\_\_\_ **3**

**Principes Fondamentaux :** \_\_\_\_\_ **3**

1. Confidentialité : \_\_\_\_\_ **3**

2. Intégrité : \_\_\_\_\_ **3**

3. Disponibilité : \_\_\_\_\_ **3**

4. Proactivité : \_\_\_\_\_ **4**

5. Responsabilisation : \_\_\_\_\_ **4**

**Mesures et Stratégies Mises en Place :** \_\_\_\_\_ **4**

Protection des infrastructures informatiques : \_\_\_\_\_ **4**

Sécurisation des accès : \_\_\_\_\_ **4**

Gestion des données sensibles : \_\_\_\_\_ **4**

Planification et réponse aux incidents : \_\_\_\_\_ **4**

Sensibilisation et formation : \_\_\_\_\_ **5**

Audit et monitoring continu : \_\_\_\_\_ **5**

**Avantages pour PEM SARL :** \_\_\_\_\_ **5**

1. Réduction des risques cybernétiques : \_\_\_\_\_ **5**

2. Confiance accrue des parties prenantes : \_\_\_\_\_ **5**

3. Optimisation des opérations : \_\_\_\_\_ **5**

4. Conformité rigoureuse : \_\_\_\_\_ **5**

**5. Préservation de la réputation : \_\_\_\_\_ 5**

# CHARTRE DE SÉCURITÉ INFORMATIQUE

La **Charte de Sécurité Informatique** de PEM SARL est une démarche stratégique visant à garantir la protection optimale des systèmes numériques et des données contre les menaces cybernétiques. Elle incarne l'engagement de l'entreprise à créer un environnement digital sécurisé, résilient et conforme aux normes réglementaires. En définissant des principes clairs et des mesures rigoureuses, cette charte est essentielle pour préserver la confidentialité, l'intégrité et la disponibilité des informations critiques de l'organisation et de ses parties prenantes.

## OBJECTIFS DE LA CHARTE :

1. **Renforcer la cybersécurité** : Protéger les infrastructures informatiques contre les cyberattaques, les intrusions et les logiciels malveillants.
2. **Maintenir l'intégrité des données** : Prévenir toute altération, destruction ou modification non autorisée des informations sensibles.
3. **Garantir la disponibilité des systèmes** : Assurer le fonctionnement continu et fiable des applications et réseaux essentiels à l'activité de PEM SARL.
4. **Respecter les réglementations** : Aligner les pratiques avec les lois et standards internationaux, renforçant ainsi la conformité légale et éthique.
5. **Former et sensibiliser** : Impliquer activement les collaborateurs dans la mise en œuvre des bonnes pratiques de sécurité.

## PRINCIPES FONDAMENTAUX :

1. **Confidentialité** : Garantir que seuls les utilisateurs autorisés ont accès aux informations sensibles.
2. **Intégrité** : Protéger l'exactitude et la fiabilité des données stockées ou transmises dans les systèmes numériques.
3. **Disponibilité** : Assurer l'accès rapide et ininterrompu aux ressources, services et outils nécessaires aux opérations quotidiennes.

4. **Proactivité** : Identifier et résoudre de manière anticipative les vulnérabilités pour minimiser les risques de violations de la sécurité.
5. **Responsabilisation** : Faire de la sécurité informatique une priorité partagée par tous les collaborateurs et partenaires technologiques.

## **MESURES ET STRATÉGIES MISES EN PLACE :**

### **Protection des infrastructures informatiques :**

- Installation de pare-feux avancés, d'antivirus et d'outils de détection d'intrusion pour surveiller et bloquer les cybermenaces.
- Segmenter les réseaux d'entreprise pour limiter la propagation des attaques potentielles.
- Mise à jour régulière des logiciels et systèmes pour corriger les failles de sécurité identifiées.

### **Sécurisation des accès :**

- Implémentation de solutions d'authentification multifactorielle (MFA) pour renforcer l'accès aux systèmes critiques.
- Génération et gestion des mots de passe complexes par des outils dédiés tels que des gestionnaires de mots de passe.
- Surveillance continue des connexions suspectes grâce à des outils d'analyse comportementale.

### **Gestion des données sensibles :**

- Application de protocoles de chiffrement avancé pour protéger les données en transit et au repos.
- Mise en œuvre de politiques strictes de classification et de traitement des données selon leur niveau de sensibilité.
- Réduction des risques liés au stockage par l'utilisation de solutions cloud conformes avec des protections robustes.

### **Planification et réponse aux incidents :**

- Élaboration d'un **Plan de Reprise d'Activité (PRA)** et d'un **Plan de Continuité d'Activité (PCA)** pour minimiser les impacts des interruptions.
- Création d'une cellule de veille et de réponse rapide pour gérer efficacement les incidents de sécurité.

- Exercices réguliers de simulation pour évaluer la capacité de l'organisation à faire face à des menaces en temps réel.

### **Sensibilisation et formation :**

- Organisation de formations périodiques pour les équipes internes sur les risques informatiques et les bonnes pratiques.
- Diffusion de guides d'utilisation sécurisée des outils numériques et des e-mails professionnels.
- Développement d'une culture d'entreprise axée sur la vigilance face aux tentatives de phishing et autres cyberattaques.

### **Audit et monitoring continus :**

- Suivi actif des performances des systèmes informatiques grâce à des tableaux de bord dédiés.
- Réalisation d'audits de sécurité réguliers pour identifier toute non-conformité ou vulnérabilité.
- Évaluation des partenaires et fournisseurs selon des normes de sécurité élevées avant toute collaboration.

## ***AVANTAGES POUR PEM SARL :***

1. **Réduction des risques cybernétiques** : Une gestion proactive des menaces minimise les risques de piratage, de perte de données ou de défaillances systèmes.
2. **Confiance accrue des parties prenantes** : Les clients, investisseurs et partenaires bénéficient d'une assurance quant à la sécurisation des informations qu'ils fournissent.
3. **Optimisation des opérations** : En maintenant la disponibilité des systèmes numériques, l'entreprise accroît son efficacité et limite les interruptions coûteuses.
4. **Conformité rigoureuse** : Une politique bien structurée garantit que PEM SARL se conforme aux exigences locales et internationales en matière de sécurité informatique.
5. **Préservation de la réputation** : En évitant les violations de données et les incidents majeurs, l'entreprise protège son image de marque et sa crédibilité.

En définitive, la **Charte de Sécurité Informatique** constitue un pilier essentiel dans la stratégie digitale de PEM SARL. Elle définit un cadre solide qui non seulement protège les systèmes et données sensibles, mais qui incarne également la responsabilité, la transparence et l'excellence opérationnelle de l'entreprise dans un contexte numérique en constante évolution.

**Le Directeur Général**

