CABINET D'EXPERTISE
EN MANAGEMENT
DES PROJETS

POLITIQUE DE CYBERSÉCURITÉ

POLITIQUE DE CYBERSÉCURITÉ

VERSION 006/07/2024/QHSE/CEMPGROUP	
Révision 17/07/2024	P/Révision 17/06/2025

Rue 87 BKK / 05 BP. : 394, Lomé (TOGO) / 00228 93077530/ 98517294
cabinetcemp2022@gmail.com / nybert86@gmail.com
www.cempconsultinggroup.com

INTRODUCTION

Le Cabinet d'Expertise en Gestion des Projets (CEMP Consulting Group) accorde une importance capitale à la sécurité de l'information et à la protection des données. Notre politique de cybersécurité vise à prévenir, détecter et répondre aux menaces cybernétiques tout en garantissant la confidentialité, l'intégrité et la disponibilité des informations.

1. Engagement pour la sécurité des informations

Nous nous engageons à :

- **Protéger les données sensibles**
  Nous garantissons la confidentialité et l'intégrité des informations grâce à des mesures de sécurité strictes, conformément à la norme ISO 27001.
- **Prévenir les cyberattaques**
  Nous mettons en place des dispositifs de sécurité avancés pour protéger notre infrastructure contre les menaces cybernétiques telles que le piratage, les virus ou le vol de données.

2. Gestion des risques cybernétiques

Nous appliquons une démarche proactive de gestion des risques cybernétiques en évaluant régulièrement les vulnérabilités et en prenant des mesures pour les atténuer :

- **Évaluation continue**
  Nous procédons à des audits réguliers de notre système informatique pour identifier les risques potentiels.
- **Plan de réponse aux incidents**
  En cas de menace ou d'attaque, nous avons un plan de réponse aux incidents permettant d'atténuer l'impact et de rétablir rapidement la sécurité des systèmes.

3. Politique de sécurité des données

CEMP Consulting Group s'assure que toutes les données traitées sont protégées contre tout accès non autorisé :

- **Accès restreint**
  Seuls les employés autorisés ont accès aux données, selon le principe du besoin de savoir.

4. Formation et sensibilisation du personnel

Nous croyons que la sécurité informatique commence par les utilisateurs. C'est pourquoi nous nous engageons à :

- **Former nos employés**
  Nous offrons des sessions régulières de formation en cybersécurité pour sensibiliser le personnel aux bonnes pratiques et aux nouvelles menaces.
- **Politique de mots de passe**
  Des règles strictes de gestion des mots de passe sont appliquées pour limiter les risques d'accès non autorisés.

5. Gestion des accès et surveillance

CEMP Consulting Group applique des politiques rigoureuses en matière de gestion des accès et de surveillance des systèmes :

- **Contrôle d'accès**
  L'accès aux systèmes d'information est sécurisé par des contrôles d'authentification multiples, y compris l'utilisation de mots de passe robustes et de l'authentification à deux facteurs.
- **Surveillance des activités**

Des outils de surveillance des activités en temps réel permettent de détecter rapidement toute anomalie ou tentative d'intrusion.

6. Protection contre les menaces externes

Notre infrastructure est protégée par des firewalls, des antivirus, et des systèmes de détection d'intrusions afin de prévenir toute menace extérieure :

- **Mises à jour régulières**
  Les systèmes et logiciels sont constamment mis à jour pour corriger les failles de sécurité et prévenir les nouvelles menaces.
- **Protection contre les malwares**
  Nous utilisons des solutions anti-malwares avancées pour détecter et éliminer toute forme de logiciel malveillant.

7. Continuité des activités

Nous avons mis en place un plan de continuité des activités pour garantir la résilience de nos opérations en cas de cyberattaque :

- **Sauvegardes régulières**
  Nous effectuons des sauvegardes quotidiennes de toutes les données critiques afin de les restaurer rapidement en cas d'incident.
- **Plan de reprise après sinistre**
  En cas d'incident grave, notre plan de reprise après sinistre permet une restauration rapide et complète des services.

8. Amélioration continue

Nous nous engageons à améliorer continuellement notre cybersécurité en intégrant les dernières technologies et en nous conformant aux nouvelles réglementations. Chaque incident est analysé pour en tirer des enseignements et améliorer nos processus.

CEMP Consulting Group s'engage à protéger ses systèmes d'information et à prévenir toute attaque ou violation de données. Notre politique de cybersécurité est un pilier central de notre engagement envers nos clients, nos partenaires et notre personnel. La direction veille à ce que toutes les ressources nécessaires soient allouées pour assurer la sécurité de nos systèmes et des informations traitées.

Responsable TIC

POYODA Pignozi

Directeur Général

NIMAN S. Martin