Best Maintenance Sarl

Votre solution technique et industrielle

CHARTE DE PROTECTION DES DONNÉES ET CYBERSÉCURITÉ

SARL au capital social de 100.000.000 GNF
RCCM/CN.TCC.2023.B.04668 - **NIF:** 421555392
Taouyah Marché, Commune de Ratoma, Conakry, République de Guinée
Tél : +224 - 622-18-65-91 / 620-45-14-85 ; **E-mail :** contact@bestmaintenance.tech
Site web: http://www.bestmaintenance.tech

03 mars 2023

Charte de Protection des Données et Cybersécurité

Introduction

La protection des données personnelles et la sécurité numérique sont des priorités fondamentales pour Best Maintenance. Conscients des enjeux liés à la confidentialité et à la cybersécurité, nous appliquons des solutions robustes permettant de garantir la confidentialité, l'intégrité et la disponibilité des informations de nos clients et partenaires. À travers cette charte, nous réaffirmons notre engagement à adopter des pratiques exemplaires pour protéger les données et maintenir un environnement numérique sûr.

Gestion des Données Clients

Principes de Confidentialité

1. Collecte Responsable

- Nous collectons uniquement les données strictement nécessaires à la prestation de nos services.
- Les données collectées sont traitées de manière transparente et avec le consentement éclairé des clients.

2. Limitation de l'Accès

- L'accès aux données clients est strictement réservé au personnel autorisé, sur la base du principe du « besoin de savoir ».
- Des contrôles d'accès basés sur des identifiants uniques et des mots de passe robustes sont en place.

3. Conservation Sécurisée

- Les informations sont stockées dans des environnements sécurisés utilisant les technologies de pointe telles que le chiffrement des bases de données.
- Les politiques de rétention limitent le stockage des données à la période nécessaire pour réaliser les objectifs fixés, conformément aux réglementations applicables.

4. Protection lors des Transferts

- Toutes les données transmises entre nos systèmes et vers des tiers sont cryptées grâce aux protocoles SSL/TLS.

Droits des Clients

- Accès et rectification des données personnelles.
- Possibilité de demander la suppression des données conformément à la réglementation en vigueur, notamment le RGPD.
- Information claire et régulière sur l'utilisation des données collectées.

Plan de Conformité RGPD et Réglementations Similaires

Engagements de Conformité

1. ***Audit Initial***
   - Analyse approfondie des traitements de données internes pour garantir leur alignement avec le RGPD et autres réglementations similaires (CCPA, LGPD).
   - Identification et suppression des collectes ou stockages de données non nécessaires.
2. ***Nomination d'un Délégué à la Protection des Données (DPO)***
   - Le DPO est responsable de veiller à l'application stricte des règles de confidentialité et assure une communication fluide avec les autorités compétentes en cas de besoin.
3. ***Mécanismes de Consentement***
   - Obtention explicite du consentement des clients pour la collecte et le traitement de leurs données.
   - Intégration d'options claires de gestion des préférences sur les plateformes numériques de l'entreprise.
4. ***Évaluation Impact sur la Vie Privée (PIA)***
   - Réalisation régulière d'analyses d'impact pour évaluer et réduire les risques liés aux traitements de données sensibles.

Bénéfices pour les Clients

- **Protection Accrue** : Les données sont protégées contre les accès non autorisés et les cyberattaques.
- **Clarté et Transparence** : Les clients sont informés précisément de l'usage de leurs données.
- **Confiance Renforcée** : L'alignement de nos pratiques avec les réglementations internationales garantit un service éthique et sécurisé.

Mesures Pratiques de Cybersécurité

1. Infrastructure Sécurisée

- **Pare-feu Sophistiqués** : Déploiement de solutions de sécurité réseau haut de gamme pour bloquer les tentatives d'intrusion.
- **Surveillance en Temps Réel** : Utilisation de systèmes de détection et de prévention des intrusions (IDS/IPS) pour identifier les menaces avant qu'elles ne causent de dommages.

2. Protocole de Sauvegarde

- **Sauvegardes Quotidiennes** : Réalisation d'une copie des données critiques chaque jour pour prévenir toute perte en cas de panne ou d'attaque.
- **Systèmes Redondants** : Implémentation de serveurs de secours géographiquement distincts pour garantir la continuité des opérations.

3. Audits et Tests de Vulnérabilité

- **Audits Récurrents** : Réalisés trimestriellement pour évaluer la robustesse de nos systèmes et identifier les failles potentielles.
- **Tests de Pénétration** : Simulation d'attaques pour évaluer la résistance des protections et améliorer les mécanismes insuffisants.

4. Formation du Personnel

- **Sensibilisation Régulière** : Sessions de formation obligatoires sur les bonnes pratiques en cybersécurité (ex. : détection de phishing, gestion des mots de passe).
- **Simulations de Crises** : Scénarios d'attaques simulées pour tester les réactions du personnel et renforcer les protocoles de réponse.

5. Gestion des Incidents

- Mise en œuvre d'un plan d'intervention rapide en cas de violation des données, comprenant :
    - Notification immédiate des parties concernées.
    - Identification et isolation de la faille pour empêcher d'autres atteintes.
    - Remédiation complète et mise à jour des systèmes exposés.

6. Collaboration avec des Experts

- Partenariats avec des sociétés spécialisées en cybersécurité pour bénéficier des dernières technologies et connaissances dans le domaine.
- Adhésion à des standards internationaux de cybersécurité, tels que l'ISO/IEC 27001.

Indicateurs de Sécurité et Résultats

Pour évaluer l'efficacité de notre politique et ajuster nos stratégies, nous suivons les indicateurs suivants :

- **Taux d'incidents de sécurité par an.**
- **Pourcentage d'employés formés sur les pratiques de cybersécurité.**
- **Durée moyenne de résolution d'une faille.**

Conclusion

La Charte de Protection des Données et Cybersécurité de Best Maintenance garantit à nos clients une gestion responsable et sécurisée de leurs données. Grâce à des politiques alignées sur les réglementations internationales et des mécanismes techniques avancés, nous assurons un environnement opérationnel fiable et conforme. Ensemble, renforçons la confiance et la transparence dans nos interactions numériques.

Le Directeur Général