Politique de sécurité de l'information

1. Objectif

Cette politique de sécurité de l'information a pour objectif de garantir la protection, la confidentialité, l'intégrité et la disponibilité des informations sensibles appartenant à l'entreprise MDR Traitements Industriels. Elle vise également à sensibiliser tous les employés, sous-traitants et parties prenantes concernées sur l'importance de la sécurité de l'information.

2. Périmètre

Cette politique s'applique à tous les employés, prestataires, consultants et tiers ayant accès aux systèmes, réseaux et données de l'entreprise MDR Traitements Industriels.

3. Classification de l'information

Toutes les informations de l'entreprise MDR Traitements Industriels doivent être classifiés en fonction de leur niveaude sensibilité. Les catégories de classification sont définies comme suit :

a) **Information Publique :** Les informations qui peuvent être partagées librement avec le public sans aucune restriction.
b) **Information Interne :** Les informations internes ne doivent pas être divulguées en dehors de l'entreprise sans autorisation.
c) **Information Confidentielle :** Les informations confidentielles sont sensibles et doivent être protégées contre tout accès non autorisé.

4. Gestion des accès

Chaque employé se voit attribuer un compte d'utilisateur individuel avec des privilèges d'accès appropriés en fonction de ses responsabilités. Les droits d'accès doivent être révisés et ajustés régulièrement, en fonction des besoins de métier et de l'évolution du personnel.

5. Sécurité des mots de passe

Les employés doivent utiliser des mots de passe complexe pour accéder aux systèmes informatiques et aux applications avec un 2FA. Les mots de passe doivent être changés régulièrement et ne doivent jamais être partagés avec d'autres personnes.

6. Utilisation appropriée des ressources informatiques

Les employés doivent utiliser les ressources informatiques de l'entreprise uniquement à des fins professionnelles autorisées. L'utilisation des systèmes informatiques à des fins illégales ou pour accéder à des informations confidentielles sans autorisation est strictement interdite.

7. Sécurité des terminaux

Tous les appareils et équipements informatiques doivent être protégés par des solutions antivirus/malware à jour. Les appareils mobiles utilisés pour accéder aux données de l'entreprise doivent être protégés par des codes PIN ou des empreintes digitales.

8. Gestion des incidents de sécurité

Toute violation de la sécurité de l'information, perte de données ou suspicion d'activités malveillantes doit être signalée immédiatement au responsable de la sécurité de l'information. Une procédure d'investigation, de gestion et de résolution des incidents de sécurité doit être mise en place.

9. Sensibilisation et formation

Tous les employés doivent suivre régulièrement des formations sur la sécurité de l'information pour être conscients des meilleures pratiques et des menaces émergentes.

10. Contrôles de conformité

Des audits réguliers seront effectués pour évaluer la conformité à cette politique et aux mesures de sécurité mises en place.

11. Sanctions

Les violations de cette politique de sécurité de l'information seront traitées de manière appropriée, conformément aux politiques disciplinaires de l'entreprise. Les sanctions peuvent aller de simples avertissements à des mesures disciplinaires plus sévères, y compris le licenciement et des poursuites légales si nécessaire.

12. Révision de la politique

Cette politique sera révisée régulièrement pour s'adapter aux nouvelles menaces et aux changements de l'environnement informatique de l'entreprise.