Bonne Pratique Relative à la Sécurité des Équipements

1. Activation du Pare-feu et de l'Antivirus :

- **Pare-feu :** Assurez-vous que le pare-feu intégré à Windows est activé. Il sert de première ligne de défense contre les intrusions malveillantes en surveillant et en contrôlant le trafic réseau entrant et sortant.
- **Antivirus :** Installez et maintenez à jour un logiciel antivirus de confiance. Configurez-le pour effectuer des analyses régulières et en temps réel pour détecter et neutraliser les menaces potentielles.

2. Chiffrement des Données :

- **BitLocker :** Activez BitLocker pour chiffrer l'intégralité du disque dur. Cela garantit que les données restent inaccessibles en cas de vol ou de perte de l'équipement.
- **Chiffrement des Fichiers Sensibles :** Pour les fichiers particulièrement sensibles, utilisez des outils de chiffrement supplémentaires pour ajouter une couche de sécurité supplémentaire.

3. Gestion des Mots de Passe :

- **Complexité des Mots de Passe :** Utilisez des mots de passe complexes, combinant lettres majuscules et minuscules, chiffres et caractères spéciaux. Évitez les mots de passe évidents ou facilement devinables.
- **Authentification à Deux Facteurs (2FA) :** Activez l'authentification à deux facteurs pour les comptes importants. Cela ajoute une couche de sécurité en demandant une deuxième forme de vérification en plus du mot de passe.

4. Mises à Jour Régulières :

- **Système d'Exploitation :** Maintenez votre système d'exploitation à jour en installant les dernières mises à jour de sécurité. Ces mises à jour corrigent les vulnérabilités connues qui pourraient être exploitées par des attaquants.
- **Logiciels et Applications :** Assurez-vous que tous les logiciels et applications installés sont également à jour. Les versions obsolètes peuvent contenir des failles de sécurité.

5. Sauvegarde des Données :

- **Sauvegardes Automatiques :** Configurez des sauvegardes automatiques régulières sur un disque dur externe ou un service de cloud sécurisé. Cela permet de récupérer rapidement les données en cas de perte ou de corruption.
- **Plan de Récupération :** Élaborez un plan de récupération en cas de sinistre pour garantir que les opérations critiques peuvent reprendre rapidement après un incident.

6. Sensibilisation à la Sécurité :

- **Formation des Utilisateurs :** Organisez des sessions de formation régulières pour sensibiliser les utilisateurs aux menaces de sécurité courantes, telles que les phishing, les ransomwares et les logiciels malveillants.

- **Politiques de Sécurité :** Établissez et communiquez clairement les politiques de sécurité de l'entreprise, y compris les bonnes pratiques pour l'utilisation des équipements et la protection des données.

7. Contrôle d'Accès :

- **Gestion des Comptes Utilisateurs :** Limitez les privilèges administratifs aux seuls utilisateurs qui en ont besoin. Utilisez des comptes utilisateurs standard pour les opérations quotidiennes.
- **Verrouillage Automatique :** Configurez le verrouillage automatique de l'écran après une période d'inactivité pour empêcher l'accès non autorisé.