



# Charte Informatique

D'une manière générale, l'utilisateur doit s'imposer le respect des lois Françaises & Européennes.

## 1) Accès au compte

L'identification permet, à chaque connexion, l'attribution des droits à chaque utilisateur sur les ressources du système.

Un identifiant (nom d'utilisateur + mot de passe) unique est confiée à chaque personne. La personne concernée assume personnellement la responsabilité de l'utilisation qui pourrait en découler et ne doit en aucun cas le divulguer.

Chaque mot de passe doit obligatoirement suivre les directives suivantes :

- Faire plus de 12 caractères,
- Inclure au moins une occurrence de type de caractères :
  - Minuscule & Majuscule
  - Chiffre
  - Spécial
- Être changé au minimum une fois toute les six mois.

## 2) Courrier électronique

Un message envoyé par Internet peut potentiellement être intercepté et lu par n'importe qui. Par conséquent, il est impératif que toute information stratégique ne soit pas échangée de cette manière, à moins qu'elle n'ait été préalablement chiffrée & que le secret ait été transmis par un autre moyen de communication.

Les messages électroniques sont conservés sur le serveur de messagerie pendant une période de 90 jours et il existe des copies de sauvegarde pendant une période de 360 jours.

Il est interdit d'utiliser des services d'intelligence artificielle pour traiter les données de l'entreprise.

### 2.1 Utilisation privée de la messagerie

L'utilisation du courrier électronique à des fins personnelles est autorisée dans des proportions raisonnables et à la condition de ne pas affecter le trafic normal des messages professionnels.

### 2.2 Contrôle de l'usage

Le contrôle porte sur :

- Nombre & destinataires des messages échangés
- Taille & contenu des messages échangés
- Format & contenu des pièces jointes

## 3) Utilisation d'Internet

Chaque utilisateur doit prendre conscience qu'il est dangereux pour l'entreprise de :

- Communiquer à des tiers des informations techniques concernant son matériel;
- Diffuser des informations sur l'entreprise sur le web
- Participer à des forums & conversations en ligne

### **3.1 Utilisation d'Internet à des fins privées**

L'utilisation d'Internet à des fins privées est tolérée dans des limites raisonnables et à condition que la navigation n'entrave pas l'accès professionnel.

### **3.2 Contrôle de l'usage**

Le contrôle porte sur :

- Durées des connexions & leurs destinations
- Fréquence des connexions & leurs date/heure

La politique et les modalités des contrôles font l'objet de discussions avec les représentants du personnel.

## **4) Pare-feu**

Le pare-feu vérifie tout le trafic entrant & sortant de l'entreprise, cherchant des sites non-autorisés, des fichiers malveillants, etc.

Il détient toutes les traces de l'activité qui transite par lui :

- Navigation sur Internet :
  - Sites visités
  - Heures des visites
  - Éléments téléchargés & leur format
- Messages envoyés et reçus :
  - Expéditeur & Destinataire(s)
  - Objet & contenu
  - Format & contenu de/des pièce(s) jointe(s)

Il filtre les URL des sites non autorisés par le principe de liste noire. Les contenus visés sont potentiellement dangereux, malveillants, inappropriés ou non conformes aux politiques de sécurité de l'entreprise.

## **5) Sauvegardes**

Le système comporte des dispositifs de protection des informations ainsi qu'un dispositif miroir destiné à doubler le système en cas de défaillance.

Ceci implique, entre autres, que la suppression par un utilisateur d'un fichier de son disque dur n'est pas absolue et qu'il en reste une copie sur :

- Dispositif de sauvegarde & miroir
- Serveur central

Fait à \_\_\_\_\_, le \_\_/\_\_/\_\_\_\_

Signature & Prénom/Nom du salarié