CHARTE INFORMATIQUE

RESPECT DES REGLES DE DEONTOLOGIE

D'une manière générale, l'utilisateur doit s'imposer le respect des lois, et notamment celles relatives aux publications à caractère injurieux, raciste, pornographique et diffamatoire sur le harcèlement sexuel/moral.

L'utilisateur ne doit pas masquer sa véritable identité ou usurper l'identité d'autrui.

Il ne doit pas effectuer d'activités pénalisant les autres utilisateurs ou son entreprise.

SECURISER L'ACCES AU COMPTE

Le contrôle d'accès logique permet d'identifier toute personne utilisant un ordinateur.

Cette identification, remise lorsque l'employé prend ses fonctions, permet, à chaque connexion, l'attribution de droits et privilèges propres à chaque utilisateur sur les ressources du système dont il a besoin pour son activité.

Une identification (login + mot de passe) unique est confiée à chaque utilisateur. Ce dernier est personnellement responsable de l'utilisation qui peut en être faite et ne doit en aucun cas la communiquer.

COURRIER ELECTRONIQUE

Les éléments de fonctionnement de la messagerie à considérer sont les suivants :

L'utilisation des moyens informatiques de l'entreprise a pour objet exclusif de mener des activités liées aux fonctions confiées dans l'entreprise.

Un message envoyé par Internet peut potentiellement être intercepté, même illégalement, et lu par n'importe qui.

En conséquence, aucune information stratégique ne doit circuler de cette manière.

Il est interdit d'utiliser des services d'un site web spécialisé dans la messagerie.

Lors du départ d'un collaborateur, il doit être indiqué au responsable de l'administration du système ce qu'il sera fait des fichiers et courriers électroniques de l'utilisateur.

Utilisation privée de la messagerie

L'utilisation du courrier électronique professionnel fournit par l'entreprise à des fins personnelles est strictement interdite.

Contrôle de l'usage

Dans l'hypothèse la plus courante, le contrôle éventuellement mis en œuvre porte sur :

- le nombre des messages échangés;
- la taille des messages échangés ;
- le format des pièces jointes.

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 ;
- connecter un micro à Internet via un modem (sauf autorisation spécifique) ;
- diffuser des informations sur l'entreprise via des sites Internet ;
- participer à des forums (même professionnels) ;
- participer à des conversations en ligne (« chat »).

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.

Contrôles de l'usage

Dans l'hypothèse la plus courante, les contrôles portent sur :

- les durées des connexions ;
- les sites les plus visités.

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

SAUVEGARDE

La mise en œuvre du système de sécurité comporte des dispositifs de sauvegarde des informations et 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 soit :

- sur le dispositif de sauvegarde ou miroir ;
- sur le serveur ;
- sur le proxy ;
- sur le firewall (pare-feu) ;
- chez le fournisseur d'accès.

Nom et Prénom(s) :

Entreprise : Start-up World
Fonction :

Fait le :

Signature de l'utilisateur :

☐ Lu et approuvé