Charte informatique de l'entreprise

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

1) Sécuriser l'accès au compte

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

Cette identification 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.

Chaque mot de passe doit obligatoirement être modifié selon la fréquence suivante : Un mot de passe doit, pour être efficace, comporter 8 caractères alphanumériques. Il ne doit pas être, notamment, identique au login, même en inversant les caractères, comporter le nom et/ou prénom de l'utilisateur ou de membres de sa famille, le numéro de téléphone, la marque de la voiture ou toute référence à quelque chose appartenant à l'utilisateur, être un mot ou une liste de mots du dictionnaire ou un nom propre, nom de lieu, être écrit sur un document et être communiqué à un tiers.

2) Courrier électronique

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

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, sauf à la crypter.

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.

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 180 jours.

Ces copies de sauvegarde conservent tous les messages au moment où ils passent sur le serveur de messagerie, même s'ils ont été supprimés ensuite par leur destinataire.

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
Dans l'hypothèse la plus courante, le contrôle éventuellement mis en œuvre porte sur :
- le nombre des messages échangés par service;
- la taille des messages échangés ;
- le format 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 ;
- de connecter un micro à Internet via un modem *(sauf autorisation spécifique)* ;
- de diffuser des informations sur l'entreprise via des sites Internet ;
- de participer à des forums *(même professionnels)* ;
- de participer à des conversations en ligne (« chat »).

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 Contrôles de l'usage
Dans l'hypothèse la plus courante, les contrôles portent sur :
- les durées des connexions par service;
- les sites les plus visités de façon globale.

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

4) Pare-feu

Le *(les)* pare-feu vérifie*(nt)* tout le trafic sortant de l'entreprise, aussi bien local que distant. Il vérifie également le trafic entrant constitué de la messagerie électronique et l'échange de fichiers, et la navigation sur Internet.

Il détient toutes les traces de l'activité qui transite par lui s'agissant :
- de la navigation sur Internet : sites visités, heures des visites, éléments téléchargés et leur nature (textes, images, vidéos ou logiciels) ;
- des messages envoyés et reçus : expéditeur, destinataire(s), objet, nature de la pièce jointe *(et éventuellement texte du message)*.

Il filtre les URL des sites non autorisés par le principe de la liste noire. Les catégories des sites visés sont les sites diffusant des données de nature pornographique, pédophile, raciste ou incitant à la haine raciale, révisionniste ou contenant des données jugées comme offensantes.

5) Sauvegardes

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

Fait à ….., le .....

Signature de l'employeur