mai 2005

GUIDE SSI
Sensibilisation du personnel

Fiche 4

MEDEF

Accompagner

La sécurité est l'affaire de chacun des employés. Une bonne politique de sécurité doit être partagée et comprise par tous. La plus grande partie des brèches de sécurité sont le fait des salariés par ignorance ou par intention frauduleuse (vol de données et transfert par Internet).

Comment se protéger ? Les 3 règles d'or de l'utilisateur.

■ **Ne pas faire confiance à un tiers** (pouvant être un manipulateur pratiquant l'« ingénierie sociale ») en n'hésitant pas à demander des justifications complémentaires et en mettant en pratique systématiquement le contre appel, même si tout laisse penser que ce tiers dispose de l'autorité nécessaire (usurpation fréquente d'identité).

■ **Préserver son identification**.

Ne communiquer (ou laisser accessible) aucun mot de passe et code d'accès personnel.

Bien choisir le mot de passe (8 caractères alpha numériques sont recommandés, sans référence à l'état civil personnel ou de personnes proches) et veiller au renouvellement tous les trois à six mois. Mais la longueur et la complexification des mots de passe ne sont pas toujours positives, les utilisateurs sont en effet souvent amenés à les noter sur un papier ou les oublient tout simplement.

En France, contrairement aux autres pays, il a été constaté en 2004 une augmentation des utilisateurs qui notent leurs mots de passe.

En moyenne sur 100 personnes, 50 écrivent le mots de passe et 35 le communiquent à un tiers ! (source étude SafeNet 2004 portant sur 67000 entreprises en France, UK, Allemagne et USA).

■ **Pratiquer librement l'autocensure**. Réserver au seul usage professionnel les moyens informatiques et le réseau de la société et accepter de limiter l'accès à certains sites et le transfert de fichiers dangereux ou de taille importante.

➔ **Eviter les téléchargements et installation sans autorisation**. Faire valider toute installation de matériel/ logiciel sur l'équipement bureautique.

➔ **Respecter les règles de connexion depuis l'extérieur**. Faire valider toute installation pouvant permettre de se connecter sur le réseau interne depuis l'extérieur du périmètre de l'entreprise.

Mise en œuvre des 3 règles. La charte d'utilisation

■ **Objectif**. La mise en place d'une Charte assure la protection du système d'information, limite la responsabilité de l'entreprise et de ses dirigeants et s'applique à tous les utilisateurs.

■ **Nature juridique**. Cette charte a une valeur d'abord informative puis normative lorsqu'elle est acceptée par le salarié. La Charte d'utilisation sera au choix :

➔ Une annexe du Règlement Intérieur (la mise en place de la Charte et sa modification suivront la procédure applicable au Règlement Intérieur),

➔ Un document unilatéral qui peut prendre la forme d'une note interne et qui répond à une procédure d'information (collective et individuelle) et de consultation mais qui renverra dans tous les cas au Règlement Intérieur de l'entreprise pour les sanctions disciplinaires applicables en cas de violation.

■ **Avis du comité d'entreprise**. La Charte doit être soumise au Comité d'entreprise pour avis conformément à l'Article L. 432-2-1 alinéa 3 du Code du travail (ou conformément à l'Article L.122-36 du Code du travail lorsque la Charte est portée en annexe du Règlement Intérieur).

■ **Contenu**. La Charte définit clairement et de façon transparente les modalités et limites de l'utilisation des moyens informatiques mis à la disposition du salarié par l'entreprise.

➔ **Protection/sécurité et confidentialité du système d'information** dont les dispositions encadrant la cybersurveillance.

- Accès au réseau sécurisé et protégé par des mots de passe accordés à un utilisateur ou à l'ensemble des utilisateurs du système d'information et confidentialité de ces derniers.

- Mise en place de pare-feux et obligation qui incombe aux responsables de les mettre à jour régulièrement.

- Obligation pour l'utilisateur d'effectuer des sauvegardes régulières afin de minimiser le risque de perte de données.

- L'introduction de tout nouveau matériel, programme ou logiciel est interdite aux utilisateurs sans autorisation de l'employeur ou de l'administrateur du système d'information.

➔ **Mise à disposition et limites d'utilisation de la messagerie** par les salariés et les institutions représentatives du personnel (dont certaines dispositions encadrant la cybersurveillance).

- Droit pour le salarié d'utiliser la messagerie électronique mise à sa disposition à des fins privées dans la limite du raisonnable,

- Obligation pour l'utilisateur de distinguer les données professionnelles des données à caractère privé,

- Possibilité pour l'employeur de sanctionner l'utilisation privée de la messagerie lorsqu'elle est abusive et compromet le fonctionnement normal de la messagerie professionnelle.

- Limitation du format, du type et de la taille des messages électroniques. La taille des messages électroniques ne devra pas venir compromettre le bon fonctionnement du système d'information et notamment sa performance,

- Possibilité pour l'employeur de modifier ces mesures par note de service.

➔ **Règles relatives à l'utilisation d'Internet**

- Mesure dans laquelle la consultation d'Internet à des fins privées est permise au salarié (une consultation raisonnable est socialement admise, la Charte ne doit pas être abusive en édictant une interdiction absolue. Cette utilisation ne doit pas venir perturber le travail du salarié ou de ses collègues),

- Interdiction de télécharger des œuvres protégées et rappel des règles selon lesquelles la responsabilité de l'employeur peut être engagée en cas de téléchargement par un utilisateur d'œuvres protégées sans l'autorisation des ayants droits (logiciel, fichiers mp3...),

- Interdiction de consulter des sites illicites (liste exhaustive des sites que l'utilisateur est en droit de consulter ou exclusion des sites contraires aux bonnes mœurs tels que les sites activistes, pédophiles ou pornographiques),

- Droit pour l'employeur, en cas de violation de cette disposition, de dénoncer l'utilisateur aux autorités compétentes,

- Interdiction de participer à des forums sauf autorisation de la direction de la communication, ou de la personne en charge de la communication de la société, pour s'exprimer au nom de cette dernière.

➔ **Contrôle**

- Droit d'accès de l'administrateur à l'ensemble des éléments du système d'information afin de le contrôler ou de le maintenir dans un souci de protection de ce dernier.

- Définition des actes de contrôle ou de maintenance du système d'information (liste exhaustive ou exclusions).

- Possibilité pour l'employeur ou l'administrateur d'exercer un contrôle sur la nature des sites visités par le salarié, la durée de connexion à Internet, les téléchargements…. Ce contrôle doit être justifié par un impératif de sécurité et de confidentialité.

- Droit pour l'employeur de conserver l'historique de messagerie électronique pendant une durée fixée dans la Charte.

➔ **Sanctions** en cas de non-respect de la Charte (Tout ce que la Charte n'interdit pas reste autorisé). Modalités d'information du salarié et procédure contradictoire en cas de sanction disciplinaire (information par écrit des griefs retenus contre le salarié, convocation écrite à un entretien, possibilité de se faire assister, déroulement de l'entretien, motivation de la sanction).

■ **Affichage et formalités - entrée en vigueur** : Lorsque la Charte est portée en annexe du Règlement Intérieur, l'employeur devra respecter les obligations suivantes :

➔ Mise en ligne de la Charte sur l'Intranet de l'entreprise,

➔ Affichage de la Charte dans l'entreprise conformément à l'Article R. 122-12 du Code du travail,

➔ Communication à l'inspecteur du travail après avis du Comité d'entreprise (ou à défaut des délégués du personnel),

➔ Dépôt de la Charte au secrétariat au greffe du Conseil des prud'hommes du siège social de la société ou de l'établissement concerné,

➔ Fixation d'une date d'entrée en vigueur, au plus tôt un mois après l'accomplissement des formalités de dépôt auprès du secrétariat au greffe et d'affichage.

■ **Litiges**. Sous peine de voir la charte remise en question par les tribunaux, le contrôle prévu par la Charte, doit être loyal, transparent et proportionné :

➔ Respect du principe de proportionnalité. Lors de la rédaction de la Charte, l'employeur doit respecter certains principes (le respect de la vie privée ou encore le principe de proportionnalité), dans le cas contraire, sa responsabilité pourrait être engagée.

➔ Information du salarié et des institutions représentatives du personnel.

■ **Assistance**.

➔ Information : Rapport de la CNIL, « La cybersurveillance sur les lieux de travail » mis à jour en février 2004 (www.cnil.fr) et Vade-mecum du MEDEF, "l'utilisation des nouvelles technologies dans l'entreprise, février 2003.

➔ Coûts de spécialistes. 3 jours d'expert (interne ou externe) dont 3 demi-journées avec l'ensemble des salariés clés suffisent à définir la charte et sensibiliser. 2 jours par an pour un diagnostic rapide et re-sensibiliser.