

CONTENU DU DOCUMENT

1 – PREAMBULE

11 - CONTEXTE

12 - UTILISATION D'INTRANET ET D'INTERNET

2 – REGLES POUR UNE UTILISATION RESPONSABLE

21 - UTILISATION DES RESSOURCES INFORMATIQUES

22 - UTILISATION D'INTRANET ET D'INTERNET

23 - CONFIDENTIALITE

3 – CONTROLE D'APPLICATION DE LA PRESENTE CHARTE

4 – MODALITES JURIDIQUES – DEPOT

ANNEXE 01 : Organisation des documents traitant de la sécurité des Systèmes d'Information

1. PREAMBULE

La présente charte est établie dans l'intérêt des utilisateurs et du Groupe, dans le respect des lois et règlements en vigueur, visés par les articles 9 du code civil et 226-15 du code pénal.

11. CONTEXTE

Le déploiement des nouvelles technologies de traitement de l'information, et en particulier celui du réseau interne, est un enjeu important pour le Groupe pour développer sa performance et sa capacité de communication, tant interne qu'externe.

Ces technologies offrent de larges possibilités d'utilisation mais leur efficacité pour le Groupe est conditionnée par la façon dont les acteurs les mettent en œuvre.

C'est pourquoi la Direction du Groupe, en concertation avec les partenaires sociaux, a convenu de formaliser les règles qui régissent l'utilisation du réseau qu'elle a mis en place.

La présente charte, annexée au règlement intérieur de chacune des entités du Groupe, est avant tout un code de bonne conduite.

Elle a pour objet de préciser les responsabilités des utilisateurs, en accord avec la législation, afin d'instaurer un usage correct des ressources informatiques du réseau, avec des règles de sécurité, de performance des moyens, de courtoisie et de respect d'autrui.

En conséquence, elle crée des obligations disciplinaires pour le personnel.

Elle a été soumise à la procédure d'adoption du règlement intérieur.

Toute violation de ses règles constituera une faute (simple, grave ou lourde au sens du Code du travail, selon les circonstances) susceptible de sanctions disciplinaires allant du simple avertissement au licenciement sans préavis ni indemnités selon sa gravité.

12. UTILISATION D'INTRANET ET D'INTERNET

Internet et Intranet sont aujourd'hui accessibles à une partie du personnel salarié du Groupe Clemessy pour ses besoins professionnels.

Au travers de son réseau Intranet, le Groupe Clemessy met à la disposition de ce personnel, depuis son poste de travail, un nouvel outil de travail permettant une communication efficace et rapide avec ses interlocuteurs tant internes qu'externes.

Aujourd'hui seuls certains postes, isolés du réseau Intranet, permettent d'accéder à Internet. Ultérieurement, sur décision de la Direction du Groupe et lorsque les dispositions sécuritaires seront mises en place, l'accès à Internet sera possible à partir d'un poste du réseau.

L'Internet et l'Intranet sont des outils de communication très performants qui offrent de nombreuses possibilités telles que : la consultation de sites, l'émission et réception de courrier électronique, la participation à des forums de discussion, le téléchargement de données et la souscription à diverses offres commerciales...

Néanmoins ces outils peuvent s'avérer une source de responsabilité si leur utilisation est détournée de sa destination professionnelle au sein du Groupe.

Tout le personnel du Groupe Clemessy doit conserver à l'esprit l'importance de l'image de marque de notre Groupe.

Chacun doit donc être conscient des responsabilités qu'il encourt et qu'il fait encourir à l'entreprise du fait d'une utilisation inappropriée des ressources des réseaux Internet et Intranet.

Par ailleurs, l'usage de la messagerie électronique, la participation à des forums, l'accès à des éléments textuels, photographiques, audio ou vidéo, et à fortiori leur téléchargement, sont susceptibles de mobiliser de manière substantielle les capacités du réseau et des postes de travail. Ces actes peuvent perturber l'utilisation par les autres personnels de cet outil de travail et par voie de conséquence l'activité du Groupe.

- ➔ **C'est pourquoi la présente charte entend fixer les lignes directrices que chacun devra comprendre et respecter.**
- ➔ **Cette charte s'applique à tout utilisateur des ressources informatiques du Groupe (salarié du Groupe, intérimaire, prestataire extérieur ou toute personne autorisée à accéder aux ressources informatiques)**

2. DES REGLES POUR UNE UTILISATION RESPONSABLE

21. UTILISATION DES RESSOURCES INFORMATIQUES

Le Groupe met à la disposition de chaque utilisateur, des équipements informatiques (infrastructure, matériels et logiciels), des moyens de communication, ainsi que des informations et données, nécessaires à l'accomplissement de sa mission.

Ces ressources sont destinées à une utilisation professionnelle, tournée vers la performance du Groupe et la satisfaction des clients.

Une utilisation personnelle de ces ressources est tolérée dans la mesure où elle remplit les conditions suivantes :

- elle présente un caractère exceptionnel
- elle n'immobilise pas les ressources mises à disposition : espace disque des serveurs, mémoire disponible, moyens d'impression et moyens de communication internes
- elle ne perturbe pas l'activité professionnelle du salarié ou de l'entreprise

Chaque utilisateur doit veiller à la conservation des ressources qu'il utilise.

A ce titre, il doit être conscient :

1. que l'utilisation de ces ressources obéit à des règles qui s'inscrivent dans le respect de la loi, de la sécurité du Groupe et du bon usage, de façon à en maintenir l'efficacité opérationnelle.
2. des conséquences d'une utilisation inappropriée des ressources informatiques : informations non protégées, postes et réseaux saturés, piratage et atteinte à la propriété intellectuelle, ...

➔ **L'utilisateur doit respecter les dispositions mises en œuvre par le Groupe pour protéger les ressources mises à sa disposition contre tout risque de destruction ou d'altération.**

Ces dispositions sont décrites dans un document **SI-116 « Règles d'utilisation des ressources informatiques »**, maintenu par la DSI (Cf. Annexe 01 de cette charte). Ce document est mis à jour au fur et à mesure de l'évolution technique des postes, des logiciels et du réseau.

Un non-respect volontaire dommageable ou un non-respect répétitif des règles inscrites dans le document SI-116, pourra selon son importance être considéré comme fautif.

22. UTILISATION D'INTRANET ET D'INTERNET

Compte tenu des risques inhérents à l'usage de l'Internet et de l'Intranet, le Groupe Clemessy appelle à la loyauté et à la responsabilité de chacun afin que l'utilisation de l'accès Internet et Intranet s'effectue dans le respect des règles élémentaires de sécurité, de précaution, de bonnes mœurs et de bonne conduite.

221. L'accès aux réseaux est mis à disposition de chaque utilisateur à des fins professionnelles.

En conséquence, chacun s'engage à s'abstenir de faire abusivement utilisation de l'accès Internet et Intranet à des fins non professionnelles.

Tout document électronique transitant par la messagerie électronique mise à disposition des salariés sera présumé revêtir un caractère professionnel. Cependant les documents qui contiendront en objet le mot « Privé » ou qui seront classés dans des répertoires ou dossiers nommés « Privé », seront considérés comme personnels

Les conditions d'accès à l'INTRANET et de son utilisation par les organisations syndicales et les I.R.P. font l'objet de dispositions spécifiques.

Seront notamment considérés comme fautifs ou abusifs, les agissements suivants :

- l'usage excessif de la messagerie électronique de l'entreprise à des fins personnelles;
- la diffusion d'informations non liées à l'activité professionnelle, en particulier les informations politiques, religieuses et sectaires ;
- la participation à des forums de discussion sans lien avec l'activité de l'entreprise ou du salarié concerné ;
- la consultation de sites et la diffusion de documents à caractère récréatif, ludique, pornographique, et plus généralement de tout site et de tout document dont l'objet est manifestement étranger à l'exercice de son activité au sein de l'entreprise ;
- La diffusion d'informations syndicales ne respectant pas le cadre des dispositions spécifiques des accords sur l'utilisation du réseau par les organisations syndicales et les I.R.P.

222. Le personnel qui ne respecterait pas les droits des tiers engagerait sa responsabilité personnelle

Le personnel doit veiller à respecter les droits des tiers, tant sur le plan du Code pénal que sur la responsabilité civile. S'il portait atteinte à ces droits à partir de son poste professionnel, il engagerait non seulement sa responsabilité personnelle mais il pourrait aussi engager la responsabilité de l'entreprise.

On distinguera deux types d'agissements fautifs ou abusifs :

- ceux qui le sont quelles que soient les circonstances
- ceux qui le deviennent quand ils ne font pas l'objet d'une autorisation expresse de l'entreprise

A - Types d'agissements considérés comme fautifs ou abusifs, en toute circonstance :

- le fait de tenir, par courrier électronique ou sur un forum de discussion, des propos xénophobes, racistes, révisionnistes ou constitutifs de harcèlement sexuel ;
- le fait de tenir, par courrier électronique ou sur un forum de discussion, des propos injurieux, diffamatoires ou dénigrants envers une personne morale ou physique ;
- le fait de communiquer, par courrier électronique ou sur un forum de discussion, des informations confidentielles ;
- la consultation de tout site proposant des contenus à caractère xénophobe, raciste, révisionniste ou des contenus pornographiques mettant en scène des personnes mineures INTERDIT PAR LA LOI;
- la diffusion de tout document illégal et en particulier les documents proposant des contenus à caractère xénophobe, raciste, révisionniste ou des contenus pornographiques mettant en scène des personnes mineures ;
- la participation à des jeux d'argent ;
- les actions d'altération volontaire de ressources informatiques :
Exemples : piratage d'un site WEB, altération du réseau (lancement de virus),
falsification de données,
- le piratage d'informations confidentielles internes ou externes

B - Types d'agissements considérés comme fautifs ou abusifs quand ils ne sont pas couverts par une autorisation expresse de l'entreprise :

- les agissements qui interviennent en **violation de dispositions légales en vigueur** (droit d'auteur, droit des bases de données...);

Exemples :

- téléchargement de logiciels ;
- téléchargement d'œuvres littéraires, cinématographiques, musicales ou photographiques

Chacun doit s'engager à la plus grande vigilance et à ne pas utiliser, reproduire, télécharger, diffuser tant à l'intérieur qu'à l'extérieur de l'entreprise d'éléments tels que logiciels, progiciels, bases de données, inventions ou créations artistiques couverts par les dispositions du code de la propriété intellectuelle et dont l'entreprise n'aurait pas légalement la disposition.

- les agissements qui **exposent l'entreprise à une mise en cause de sa responsabilité**

Exemple : la commande en ligne de tous produits et services ;

- les agissements qui **divulguent des informations ou documents appartenant au Groupe ou à l'un de ses clients ou partenaires**

Exemples :

- la communication à un tiers extérieur au Groupe de l'adresse e-mail d'une personne sans une autorisation expresse de celle-ci ou d'un carnet d'adresses du Groupe,
- la communication des documents d'un client à un tiers non autorisé,
- la participation à des forums techniques.

23. CONFIDENTIALITE

- Les mots de passe d'accès aux réseaux, logiciels et données sont confidentiels et permettent l'identification de l'utilisateur. Ils ne doivent pas être divulgués à des tiers internes ou externes.
- Tout utilisateur doit respecter la confidentialité de la messagerie. Seront considérés comme fautifs ou abusifs les agissements consistant notamment à
 - se faire passer pour une autre personne,
 - modifier le message d'un tiers,
 - envoyer un message anonyme,
 - utiliser une adresse non autorisée,
 - utiliser la boîte aux lettres d'autrui, sans procuration formelle.
- Sauf pour les besoins de contrôle décrits dans le chapitre suivant, l'employeur s'engage à ne pas prendre connaissance, sans son autorisation expresse, des messages envoyés ou reçus par le personnel en activité dans le Groupe.

Nota : Sur Internet, la confidentialité des données ne peut pas être assurée par l'entreprise

3. CONTROLE D'APPLICATION DE LA PRESENTE CHARTE

→ Le Groupe Clemessy est amené à mettre en place des procédures de contrôle

Afin de garantir l'effectivité des principes définis dans la présente charte et d'assurer la sécurité de son réseau interne, le Groupe Clemessy pourra être amené à mettre en oeuvre certains contrôles sur l'utilisation par ses employés et par des tiers extérieurs de l'accès à Internet et à l'Intranet, ou de façon plus générale, aux ressources informatiques du Groupe.

Ces contrôles s'effectueront **dans le respect du droit à la vie privée de chacun.**

Les **contrôles automatiques** mis en oeuvre par le Groupe Clemessy pourront porter sur :

- l'identification des sites consultés par les utilisateurs,
- l'origine des messages reçus,
- la durée de connexion,
- le volume des messages échangés par utilisateur,
- la fréquence et la taille des messages échangés,
- le nombre des destinataires,
- le format des pièces jointes,
- la présence de facteurs représentatifs des agissements tels que décrits dans le § 222 - A, dans le contenu des messages électroniques adressés et reçus par les utilisateurs, les sites consultés ou les services utilisés.

Conformément à l'article 27 de la loi "Informatique et Libertés" n° 78-17 du 6 janvier 1978, les utilisateurs des ressources informatiques du Groupe sont informés que les informations collectées par les serveurs font ou feront l'objet de traitements automatisés :

sauvegardes, contrôle de la nature et des volumes des documents stockés ou véhiculés par le réseau, archivages et purges, contrôle des accès, contrôle de la nature des sites consultés et des sites émetteurs d'informations entrantes, contrôle de présence et éradication de virus et de tous les moyens d'attaque de nos ressources informatiques.

Seuls le Directeur des Systèmes d'information, l'Agent de sécurité titulaire du Groupe et l'Agent de sécurité informatique du Groupe auront accès aux informations collectées par l'infogérant ou les fournisseurs d'accès à Internet, habilités contractuellement et engagés confidentiellement à opérer pour notre compte.

Chacun dispose d'un droit d'accès aux informations qui le concernent : ce droit s'exerce auprès de l'Agent de sécurité titulaire du Groupe et l'Agent de sécurité informatique du Groupe.

En cas de présomption d'utilisation abusive ou frauduleuse de la messagerie et des ressources informatiques du Groupe, l'employeur pourra

- d'une part demander au salarié concerné qu'il justifie du caractère professionnel de l'utilisation qu'il en a faite ou de toute autre circonstance justificative ;
- d'autre part prendre toute mesure pratique de nature à établir légalement la faute du salarié (listing des messages, des documents et des sites incriminés, constat d'huissier, ...)

En cas de prévision de sanction d'un salarié liée à un non-respect de cette charte, une commission, composée d'un représentant par organisation syndicale représentative, sera réunie pour analyser avec la Direction les raisons de cette éventuelle sanction. Cette commission fonctionnera jusqu'au 31 décembre 2004.

4. MODALITES JURIDIQUES – DEPOT

Après consultation des instances représentatives du personnel, et avis de l'inspection du travail du siège respective de chaque Société composant le Groupe, la charte est affichée dans chaque entreprise et déposée aux greffes des Conseils de prud'hommes concernés territorialement.

Cette annexe au règlement intérieur entrera en **application le 15.05.2003** dans la Société Clemessy SA.

Le document est **disponible dans le Référentiel** du Groupe.

Quatre niveaux de documents peuvent traiter de la sécurité des systèmes d'information :

Niveau 1 : **Un document général** qui reprend les grands principes auxquels le Groupe est attaché.
C'est un document collectif, annexé au règlement intérieur de chaque Société, dont le contenu n'évolue pas dans le temps.
C'est la « Charte d'Utilisation des ressources informatiques » codifiée SI -110

Niveau 2 : **Des documents spécifiques plus détaillés** qui déclinent les principes pratiques de mise en application de la charte générale. Ce sont des documents qui évoluent avec les techniques et les outils disponibles dans le Groupe, avec les possibilités financières du Groupe et en fonction des négociations avec les partenaires sociaux.
Ces documents sont collectifs et doivent toujours rester conformes à la charte générale.

Niveau 3 : **Des procédures d'application** qui décrivent comment doivent être mises en œuvre certaines dispositions décrites dans les documents de niveau 2.
Leur application est obligatoire et contrôlable (système qualité).

Niveau 4 : **Des documents individuels** qui concernent le personnel extérieur ou temporaire, le personnel ayant un droit d'accès général à INTERNET à partir d'un poste du réseau, le personnel ayant des droits particuliers (travail sur des marchés classés, administrateurs, ...)

