CHARTE UTILISATEUR

TYPE DE DOCUMENT	Politique de sécurité		
DOMAINES D'APPLICATIONS	Sécurité du système d'information Informatique & Qualité		
CLASSIFICATION DES INFORMATIONS ET DU DOCUMENT	Interne		
	☐ Sensible ☑ Confidentiel (interne) ☐ Confidentiel (partenaires) ☐ Restreint ☐ Public		
RÉFÉRENCE			
VERSIONS	N°	MODIFICATIONS	DATES
	1.0	Publication	XX/XX/XX
	1.1	Rectification	XX/XX/XX
	1.2	Rectification	XX/XX/XX
	2.0	Evolution pour	XX/XX/XX
	2.1	Evolution pour	XX/XX/XX
DESCRIPTION	La charte utilisateur est un code de bonne conduite pour l'usage des ressources informatiques et des services Internet. Elle concerne les documents à destination de l'ensemble du personnel utilisant le système d'information de l'entreprise et formalise la responsabilité de ces utilisateurs en accord avec la législation en vigueur.		
RÉDACTEURS	NOM	SOCIÉTÉ	
	Rédacteur 1	La Société	
	Rédacteur 2	La Société	
DIFFUSION	NOM	SOCIÉTÉ	POUR
	X	La Société	Révision
	X	La Société	Révision

TABLES DES MATIÈRES

1.INTRODUCTION

1.1.OBJET

Ce texte, associé au règlement intérieur de La Société, est avant tout un code de bonne conduite. Il a pour objet de préciser la responsabilité des utilisateurs en accord avec la législation afin d'instaurer un usage correct des ressources informatiques et des services Internet, avec des règles minimales de courtoisie et de respect d'autrui.

Pour tout renseignement complémentaire, vous pouvez vous adresser au Comité de Direction.

1.2.DÉFINITIONS

On désignera de façon générale sous le terme " ressources informatiques ", les moyens informatiques ainsi que ceux auxquels il est possible d'accéder à distance, directement ou indirectement à partir du réseau administré par La Société.

On désignera par " services Internet ", la mise à disposition par des serveurs locaux ou distants de moyens d'échanges et d'informations diverses : Web, messagerie, forum…

On désignera sous le terme " utilisateur ", les personnes ayant accès ou utilisant les ressources informatiques et services Internet.

On désignera sous le terme " entité " les entités créées par La Société pour l'accomplissement des missions des utilisateurs.

On désignera sous le terme " Direction" un des membres du Comité de Direction de La Société.

1.3.CHAMP D'APPLICATION

La présente charte s'applique à l'ensemble des personnes, permanentes ou temporaires, utilisant les moyens informatiques internes de La Société ainsi que ceux auxquels il est possible d'accéder à distance directement ou en cascade à partir du réseau administré par La Société. La charte ne s'applique pas aux clients ou aux utilisateurs des sites et services fournis par La Société à travers Internet.

La présente charte sera annexée, à titre d'information, aux contrats de travail conclus avec les utilisateurs contractuels qui auront accès au système informatique de leur entité.

Elle sera en outre signée par toute personne accueillie au sein de La Société et ayant régulièrement accès au dit système.

2.ACCÈS AUX RESSOURCES INFORMATIQUES ET SERVICES INTERNET

L'utilisation des ressources informatiques et l'usage des services Internet ne sont autorisés que dans le cadre exclusif de l'activité professionnelle des utilisateurs conformément à la législation en vigueur.

L'activité professionnelle est celle prévue par les statuts de salarié de l'utilisateur, mais également toute activité administrative et de gestion découlant ou accompagnant ces activités.

L'utilisation des ressources informatiques partagées de l'entité et la connexion d'un équipement sur le réseau sont en outre soumises à autorisation. Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Ces autorisations peuvent être retirées à tout moment. Toute autorisation prend fin lors de la cessation même provisoire de l'activité professionnelle qui l'a justifiée.

L'entité pourra en outre prévoir des restrictions d'accès spécifiques à son organisation : Carte à puce d'accès ou d'authentification, filtrage d'accès sécurisé etc.

2.1.DEVOIRS D'UTILISATION, DE SÉCURITÉ ET DE BON USAGE

Tout utilisateur est responsable de l'usage des ressources informatiques et des services internet auxquels il a accès. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale et à celle de son entité.

L'utilisation de ces ressources doit être rationnelle et loyale afin d'en éviter la saturation ou leur détournement à des fins personnelles.

En particulier l'utilisateur :

- Doit appliquer les recommandations de sécurité de l'entité à laquelle il appartient,
- Doit assurer la protection de ses informations et il est responsable des droits qu'il donne aux autres utilisateurs, il lui appartient de protéger ses données en utilisant les solutions de sauvegarde en ligne, lorsqu'elles sont mises à sa disposition,
- Doit signaler toute tentative de violation de son compte et, de façon générale, toute anomalie qu'il peut constater,
- Doit suivre les règles en vigueur au sein de l'entité pour toute installation de logiciel,
- Choisit des mots de passe sûrs, gardés secrets et en aucun cas ne doit les communiquer à des tiers,
- S'engage à ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux, à travers des matériels dont il a l'usage,
- Ne doit pas utiliser ou essayer d'utiliser des comptes autres que le sien ou de masquer sa véritable identité,
- Ne doit pas tenter de lire, modifier, copier ou détruire des données autres que celles qui lui appartiennent en propre, directement ou indirectement. En particulier, il ne doit pas modifier le ou les fichiers contenant des informations comptables ou d'identification,
- Ne doit pas quitter son poste de travail ni ceux en libre-service sans se déconnecter en laissant des ressources ou services accessibles,
- Ne doit pas publier ou permettre l'accès, directement ou indirectement aux codes sources et documents internes auxquels il a accès sans accord préalable de la direction.
- Ne doit pas, d'une manière générale, utiliser son téléphone professionnel (portable ou fixe) ou privé, pour un usage personnel (communications vocales, messages textes ou autre), pendant les heures de bureau, même si une tolérance sera appliquée au cas par cas,
- Aucun raccordement au réseau local (bureau, via réseau sans fil ou réseau filaire…) d'un équipement autre que celui fourni par La Société ne sera toléré, sauf approbation exceptionnelle par la direction.

2.2.RÈGLES DE CONFIDENTIALITÉ

2.2.1.Procédures d'accès aux informations

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leur sont propres, et ceux qui sont publics ou partagés. En particulier, il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées.

Cette règle s'applique également aux conversations privées de type courrier électronique dont l'utilisateur n'est destinataire ni directement, ni en copie.

Elle s'applique aussi aux conversations téléphoniques. Il n'est pas autorisé de consulter une messagerie vocale d'un collègue, ou de transmettre le contenu d'une conversation privée par quelque moyen que ce soit.

Si, dans l'accomplissement de son travail, l'utilisateur est amené à constituer des fichiers tombant sous le coup de la loi Informatique et Libertés, il devra auparavant en avoir fait la demande à la CNIL en concertation avec le Directeur de l'entité et en avoir reçu l'autorisation.

Il est rappelé que cette autorisation n'est valable que pour le *traitement* défini dans la demande et pas pour le *fichier* lui-même.

Tous les documents et supports contenant des données sensibles (document de sécurité et sauvegardes notamment), vitales ou nominatifs doivent être systématiquement rangés dans une armoire ou un local fermé à clés et accessible par les personnes habilitées.

2.2.2. Procédures de diffusion des informations

Les informations sensibles et vitales ne peuvent être diffusées en interne à des personnes autres que les propriétaires de l'information, les utilisateurs habilités ou autres que celles explicitement indiquées sur les supports, qu'avec l'accord de la Direction.

Les informations sensibles et vitales ne peuvent être diffusées à l'extérieur de l'entreprise qu'avec l'accord de la Direction et l'habilitation du destinataire.

Les informations internes ne peuvent être diffusées à l'extérieur de l'entreprise qu'avec l'accord de la Direction et l'habilitation du destinataire.

Les informations nominatives ne peuvent être diffusées qu'en accord avec la loi (cf. chapitre 4.1).

Les supports (disque dur, clé USB…) contenant ou ayant contenus des informations sensibles, vitales ou nominatives doivent être physiquement effacées s'ils doivent être réutilisés ou détruits ou rendus physiquement inutilisable avant leur mise au rebut.

2.2.3.Procédures de protection par mot de passe

Procédures à appliquer :

- Les mots de passe vides sont interdits,
- Le mot de passe doit avoir une longueur minimale de 8 caractères,
- L'utilisation partielle ou totale de mot issu d'un dictionnaire, de noms propres ou d'informations à caractère personnel (nom ou prénom avec une date de naissance par exemple) est interdite,
- Le mot de passe doit être un mélange d'au moins une majuscule ([a-z]), au moins une minuscule ([a-z]), d'au moins un chiffre ([0-9]) et au moins un caractère spécial tel que « #, ;:!?@ »,
- Un mot de passe ne doit pas réutiliser tout ou partie d'un ancien mot de passe,
- Un mot de passe ne doit pas pouvoir se déduire du précédent (janvier puis février par exemple).
- Un mot de passe doit avoir une période de validité de 72 jours maximum

2.2.4.Procédures de protection physique

Tout vol d'un équipement appartenant à La Société (ordinateur portable, matériel contenant des données propriété de l'entreprise…) doit être signalé à la Direction.

2.3.RÈGLES D'USAGE DES SERVICES INTERNET

2.3.1.Procédures d'accès à partir du réseau interne

L'utilisateur doit faire usage des services Internet dans le cadre exclusif de ses activités professionnelles et dans le respect de principes généraux et des règles propres aux divers sites qui les proposent ainsi que dans le respect de la législation en vigueur.

En particulier l'utilisateur :

- Ne doit pas se connecter ou essayer de se connecter sur un serveur autrement que par les dispositions prévues par ce serveur ou sans y être autorisé par les responsables habilités,
- Ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède,
- Ne doit pas usurper l'identité d'une autre personne et ne doit pas intercepter de communications entre tiers,
- Ne doit pas utiliser ces services pour proposer ou rendre accessible aux tiers des données et informations confidentielles ou contraires à la législation en vigueur,
- Ne doit pas déposer des documents sur un serveur sauf si celui-ci le permet ou sans y être autorisé par les responsables habilités,
- S'interdit l'utilisation de modems au sein de l'entreprise autres que ceux dûment identifiés,
- S'interdit l'utilisation d'équipements wifi au sein de l'entreprise autres que ceux dûment identifiés.

L'entité ne pourra être tenue pour responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne se sera pas conformé à ces règles.

2.3.2.Procédures d'accès au réseau interne par un accès externe

Procédures de connexion au travers du réseau de l'opérateur :

- L'utilisateur s'engage à respecter les règles d'utilisation de ce type d'accès particulièrement en cas de perte des éléments de sécurité (jeton, identifiant, …),
- L'utilisateur utilise exclusivement un mécanisme d'identification et d'authentification pour se connecter,
- L'utilisateur limite l'utilisation de ses connexions au réseau privé d'entreprise au strict nécessaire.

Procédures d'utilisation du réseau internet au domicile à partir d'un portable de l'entreprise :

- Les derniers correctifs des systèmes d'exploitation et des logiciels sont installés sur le portable conformément aux recommandations de la cellule sécurité de l'entreprise,
- L'antivirus doit être actif et à jour des signatures,
- Le portable dispose d'un système de protection personnel qui interdit toutes les tentatives de connexions, ou est protégé par un système de filtrage,

- L'utilisateur a été sensibilisé aux risques de sécurité et au respect du secret professionnel, de la propriété intellectuelle, et des droits d'auteur,
- L'utilisateur connaît la classification des informations ainsi que les règles de diffusion de celles-ci.

Procédures d'accès aux serveurs de messagerie de l'entreprise depuis un poste public en libre-service (type cybercafé) :

- L'utilisateur tient compte des risques de sécurité et du respect du secret professionnel, de la propriété intellectuelle, et des droits d'auteur,
- L'utilisateur connaît la classification des informations ainsi que les règles de diffusion de celles-ci.
- Note : tout accès aux serveurs de l'entreprise (autre que le serveur de messagerie) depuis un poste public en libre-service (type cybercafé) est interdite.

2.3.3. Règles d'accès à Internet : Web

L'utilisation du Web pour usage personnel n'est autorisée qu'en dehors des heures de travail et à condition de ne pas perturber le réseau de La Société.

Pour canaliser cet usage, La Société se réserve le droit de mettre en place la politique de filtrage qu'elle jugera appropriée, tout en informant ses collaborateurs au préalable.

L'utilisateur qui accède à des sites Web :

- Doit s'imposer le respect des lois en s'interdisant l'accès aux sites à caractère injurieux, raciste, pornographique ou diffamatoire,
- Doit considérer toute information provenant d'un site web comme étant, à priori sujette à caution : pour utiliser une information provenant de site web dans un usage professionnel, il est nécessaire de la recouper avec d'autres sources d'informations,
- Ne doit jamais utiliser de programmes de partage de fichiers « peer-to-peer » (ex : kazaa, emule, etc…),
- Ne doit pas compromettre, par un usage immodéré, l'accès à internet pour les autres utilisateurs,
- Ne doit pas recevoir et installer de fichiers ou de programmes venant de sites web non validés,
- Doit limiter l'usage de ressources dites « en streaming » aux seuls besoins professionnels.

2.3.4. Règles d'usage de la messagerie, des forums et des chats

Les outils de communication, incluant la messagerie, les forums professionnels de discussion et les chats sont des outils professionnels importants d'usage quotidien à l'intérieur de La Société.

Dans ce cadre, l'utilisateur :

- Doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques par courrier, forums de discussions : c'est la netiquette : charte de bonne conduite des acteurs de l'Internet, qu'ils soient utilisateurs professionnels ou particuliers (Cf : http://netiquette.afa-france.com/),
- N'émettra pas d'opinions personnelles étrangères à son activité professionnelle susceptibles de porter préjudice à La Société,
- Doit informer sa hiérarchie s'il reçoit un message ou des propos d'un de ses collègues, ne correspondant pas à ces règles.

La messagerie doit être principalement réservée à l'usage professionnel, elle ne doit pas être utilisée au détriment des intérêts de La Société.

La messagerie n'est pas un système intrinsèquement sécurisé, il est donc important d'être très vigilant quant à l'usage qui en est fait, spécialement avec les documents qui peuvent avoir un caractère confidentiel.

La messagerie de La Société ne doit pas être utilisée par des personnes ne faisant plus partie de l'entreprise.

Dans le cadre particulier de la messagerie, l'utilisateur :

- Ne doit pas s'enregistrer avec son adresse professionnelle, sur des sites Web à usage personnel,
- Ne doit pas rediriger automatiquement sa réception de messages sur une boite aux lettres personnelle,
- Doit vérifier que sa boîte aux lettres n'excède pas la taille maximum qui lui a été allouée : il doit, pour se faire, effectuer régulièrement des sauvegardes de ses anciens messages,

- Ne doit pas envoyer des messages qui dépassent la taille maximum prescrite, il peut compresser les fichiers liés en utilisant uniquement les programmes de compression recommandés,
- Ne prend en compte que les messages d'alerte provenant du service informatique,
- N'envoie des messages de diffusion générale qu'après en avoir reçu l'autorisation de son management en fonction des critères et explications (cause, date, périmètre de la distribution) qu'il fournira,
- Ne doit pas en faire un usage immodéré, en fréquence et en volume, durant les heures de travail : le non-respect de cette consigne peut déclencher des actions disciplinaires,
- Ne doit jamais envoyer d'informations liées à des « copyright » tiers : ceci est assimilé à une faute lourde pouvant avoir des conséquences pénales.

2.4.RÈGLES DE PRÉSERVATION DE L'INTÉGRITÉ DES SYSTÈMES INFORMATIQUES

L'utilisateur s'engage à ne pas apporter volontairement de perturbation au bon fonctionnement des systèmes informatiques et des réseaux, que ce soit par des manipulations anormales du matériel, ou par l'introduction de logiciels parasites connus sous le nom générique de virus, chevaux de Troie, bombes logiques....
Tout travail risquant de conduire à la violation de cette règle, ne pourra être accompli qu'avec l'autorisation du responsable de l'entité et dans le strict respect des règles qui auront alors été définies.

2.4.1.Procédures de sécurité collective

L'utilisateur est tenu de participer à la sécurité du système (choix de bon mot de passe, signalement de tout problème de sécurité, respect et application des consignes de l'administrateur...)

Pour la sécurité collective, l'utilisateur ne tentera pas :

- De masquer sa véritable identité,
- De modifier ou détruire des informations ou de porter atteinte à l'intégrité de tout système connecté ou non au réseau,
- D'interrompre ou de dégrader le fonctionnement du réseau,
- De se connecter ou d'essayer de se connecter sur un site sans y être autorisé ou de chercher à porter atteinte à d'autres sites,
- D'effectuer des expérimentations sur la sécurité des systèmes informatiques et réseaux, ni sur les virus sans autorisation préalable,
- De développer, installer ou détenir un programme ayant les propriétés décrites ci-dessous :
    - Programmes cherchant à contourner la sécurité d'un système,
    - Programmes contournant les protections des logiciels.

2.4.2.Procédures de protection antivirale

Procédures d'utilisation du poste de travail :

- L'utilisateur vérifie qu'un logiciel antivirus est installé sur son poste de travail, qu'il est actif et que ses mises à jour sont bien appliquées,
- Les postes de travail des utilisateurs doivent être protégés après un délai d'inactivité par l'utilisation d'un écran de veille qui se déclenche au bout de 10 minutes et protégé par un mot de passe,

Procédures d'utilisation de la messagerie :

- Les messages provenant d'un expéditeur inconnu ou incertain doivent obligatoirement être supprimés sans ouvrir aucune pièce jointe,
- Les messages qui paraissent étranges ou non conventionnels doivent obligatoirement être supprimés même si l'expéditeur est connu (un ami ou un collègue),
- En cas de doute sur le contenu d'un message expédié par une personne connue (interne ou externe), demander une confirmation à l'expéditeur qu'il a bien envoyé le message,
- Ne jamais rediriger ou répondre à un message non désiré (spam) même pour se « désinscrire » d'une liste,

- Les réponses automatiques aux messages lors de périodes d'absences (vacation message) ne sont autorisées que pour les adresses internes.

Procédures d'utilisation des téléchargements :

- L'utilisation de logiciels qui n'a pas vocation à servir une cause liée à un projet professionnel en cours ou à venir est interdite.

Conduite à tenir en cas de détection d'incident :

- Tout poste de travail infecté ne pourra être reconnecté au réseau de l'entreprise qu'après contrôle et validation (éradication du virus) de l'équipe informatique,
- En cas de détection d'un virus dans un message, prévenir la ou le correspondant sécurité de l'établissement,
- En cas de détection d'un canular (hoax) dans un message, ne pas le retransmettre et prévenir l'équipe informatique.

2.4.3. Procédures de protection à l'extérieur du site

Les équipements informatiques peuvent être utilisés à l'extérieur du site (connectés au réseau Internet ou aux réseaux des clients) dans les conditions suivantes :

- Les équipements doivent être installés et configurés conformément aux standards de La Société, notamment en ce qui concerne l'antivirus (actif et à jour des signatures),
- L'accès aux ressources de l'équipement n'est possible qu'après identification et authentification de l'utilisateur conformes aux procédures de gestion des mots de passe,
- Si l'équipement dispose d'informations sensibles, vitales ou nominatives :
    - L'utilisation à l'extérieur doit faire l'objet d'un accord du propriétaire des informations,
    - Les données doivent préalablement avoir été enregistrées sur un serveur de fichiers interne,
    - L'utilisateur est responsable des sauvegardes des données modifies à l'extérieur de l'entreprise,
    - Les interfaces de communication sans-fil doivent être désactivées,
- Les équipements installés doivent se conformer aux procédures de connexion externes,
- L'utilisateur est responsable de la protection de l'équipement et des données qu'il contient dès lors qu'il l'utilise à l'extérieur de l'entreprise,
- L'utilisateur doit respecter les chartes, politiques ou règles de sécurité en vigueur chez les clients chez qui il intervient.

2.5. Respect de la législation concernant les logiciels

L'utilisateur ne peut installer un logiciel qu'après avis de son supérieur hiérarchique.

L'utilisateur ne doit pas installer ou utiliser des logiciels dont les droits de licence n'auraient pas été honorés. De plus il ne doit jamais contourner les restrictions d'utilisation d'un logiciel.

Il est strictement interdit d'effectuer des copies de logiciels commerciaux pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle. Ces dernières ne peuvent être effectuées que par la personne habilitée à cette fin par le responsable de l'entité.

Par ailleurs l'utilisateur ne doit pas installer de logiciels à caractère ludique, ni contourner les restrictions d'utilisation d'un logiciel.

2.6.DROITS ET DEVOIRS SPÉCIFIQUES DES ADMINISTRATEURS SYSTÈMES ET/OU RÉSEAUX

Les administrateurs systèmes et/ou réseaux sont informés des implications légales de leur travail, en particulier des risques qu'ils courent dans le cas où un utilisateur du système dont il a la charge commet une action répréhensible.
Le BYOD est interdit :

- Toute utilisation d'un dispositif informatique (poste de travail / laptop / tablette / téléphone mobile) personnel est prohibé.
- Toute copie d'information propriété de La Société, ou un de ses clients, sur un support appartenant à un collaborateur est prohibé.

Tout administrateur systèmes et/ou réseaux a le droit :

- D'accéder, sur les systèmes ou le réseau qu'il administre, aux informations nécessaires à des fins de diagnostic et d'administration du système ou du réseau, en respectant scrupuleusement la confidentialité de ces informations et en s'efforçant de ne pas les altérer,
- D'établir des procédures de surveillance de toutes les tâches exécutées sur les machines, afin de déceler les violations ou les tentatives de violation de la présente charte,
- De prendre, en cas d'infraction à la charte, des mesures conservatoires, si l'urgence l'impose, sans préjuger des sanctions qui pourraient en résulter.

Tout administrateur systèmes et/ou réseaux a le devoir :

- D'informer les utilisateurs, de les sensibiliser aux problèmes de sécurité informatique et de leur faire connaître les règles de sécurité à respecter,
- De configurer et administrer le système ou le réseau dans le sens d'une meilleure sécurité,
- De respecter les règles de confidentialité, en limitant l'accès aux informations strictement nécessaires et en respectant le « secret professionnel ».

Tout administrateur devant accéder à une ressource informatique aux fins de maintenance :

- Doit protéger ses accès par un mot de passe respectant la politique de gestion de mots de passe (longueur, robustesse, expiration, …)
- Doit utiliser, dans la mesure du possible, des protocoles sécurisés pour configurer les équipements à distance,
- Doit limiter les accès de maintenance depuis l'extérieur de l'entreprise et doit contrôler l'utilisation des ressources

Pour des nécessités de maintenance et de gestion technique, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect de la législation applicable et notamment de la loi sur l'informatique et les libertés.

L'enregistrement de l'utilisation des ressources informatiques et des services internet a pour objectif de permettre :

- L'analyse des causes et des origines des intrusions et des utilisations frauduleuses,
- Le contrôle de l'application de la Politique de sécurité de La Société pour l'usage des services Internet (Messagerie, Web),
- La vérification des habilitations pour l'accès aux ressources essentielles de l'entreprise.

L'usage des ressources suivantes est tracé :

- L'usage de l'Internet (Web) par les utilisateurs du système d'information,
- L'usage de la messagerie par les utilisateurs du système d'information,
- Les connexions et les accès réussis ou ratés,
- Les connexions aux accès à une ressource informatique aux fins de maintenance.

3.RAPPEL JURIDIQUE

3.1.LOIS APPLICABLES

Il est rappelé que toute personne sur le sol français doit respecter la législation française en particulier dans le domaine de la sécurité informatique :

- La loi du 6/1/78 dite "informatique et liberté",

(cf. Http://www.cnil.fr/)

- La législation relative à la fraude informatique, (article 323-1 à 323-7 du code pénal),

(cf. Http://www.legifrance.gouv.fr/citoyen/code.cgi)

- La législation relative à la propriété intellectuelle

(cf. Http://www.legifrance.gouv.fr/citoyen/code.cgi)

- La loi du 04/08/1994 relative à l'emploi de la langue française,

(cf. Http://www.culture.fr/culture/dglf/)

- La législation applicable en matière de cryptologie.

(cf. Http://www.telecom.gouv.fr/francais/activ/techno/crypto0698_1.htm)

3.2.RAPPEL SUR LA PROPRIÉTÉ INTELLECTUELLE

La reproduction, la représentation ou la diffusion d'une œuvre de l'esprit ou d'une création protégée au titre de droits voisins est soumise au respect des droits de propriété intellectuelle et nécessite une cession et/ou une autorisation émanant des titulaires des droits patrimoniaux et moraux prévus par le Code de la Propriété intellectuelle, sous peine de constituer le délit de contrefaçon de droit d'auteur.

De même, les signes distinctifs et inventions étant susceptibles de protection au titre d'un droit de propriété intellectuelle, leur reproduction, représentation ou diffusion est susceptible de constituer, à défaut de telles cessions et/ou autorisations, le délit de contrefaçon de marque ou de brevet.

En ce qui concerne plus particulièrement la reproduction et/ou l'utilisation d'un logiciel, il est rappelé qu'en l'absence d'autorisation du titulaire des droits de propriété intellectuelle sur ce logiciel ou en cas de non-respect des conditions et limites définies par celui-ci (en ce qui concerne notamment les copies de sauvegarde), cette reproduction et/ou utilisation peut également être constitutive du délit de contrefaçon.

Il est enfin rappelé que les bases de données sont protégées au bénéfice de leur auteur.

3.3.SANCTIONS

Tout utilisateur n'ayant pas respecté les règles définies dans la présente charte est passible d'interdiction d'accès au réseau, de fermeture immédiate de son compte, de sanctions internes à La Société et/ou de poursuites judiciaires selon le cas.

Fait à , le en deux exemplaires.

Signature du salarié