CHARTE INFORMATIQUE

Préambule

La société ……., met en œuvre un système d'information et de communication nécessaire à son activité, comprenant notamment un réseau informatique et téléphonique.

Les salariés, dans l'exercice de leurs fonctions, sont amenés à utiliser ces moyens mis à leur disposition.

Cette charte a pour objectif de :

a) Sensibiliser les utilisateurs sur les risques d'une mauvaise utilisation, incontrôlée ou non-sécurisée, au détriment de l'entreprise, tels que :

- Le piratage des données numériques
- Les attaques virales
- Le préjudice à l'image de l'Entreprise
- La divulgation non désirée de données confidentielles
- La détention ou diffusion de données contraire à la loi
- Le non respect des obligations du R.G.P.D

b) Informer formellement l'utilisateur

c) Permettre, dans le cadre de la loi, les contrôles nécessaires au bon usage des systèmes informations.

Dans un but de transparence à l'égard des utilisateurs, la présente charte pose les règles relatives à l'utilisation de ces ressources de communication de la Société.

1 Champ d'application

1.1 Système d'information et de communication

Le système d'information et de communication de l'entreprise est notamment constitué des éléments suivants:

- ordinateurs (fixes ou portables),
- périphériques de sauvegarde,
- photocopieurs,
- téléphones,
- serveurs,
- espace WEB,
- messagerie,
- Logiciels métier,
- services en ligne,
- données et bases de données,

(ci-après désignés collectivement par le terme « e-Ressources »).

Les e-Ressources de la Société sont fournies en vue d'être utilisées uniquement pour des buts professionnels légitimes et en conformité avec les politiques, procédures, directives et instructions en vigueur dans la Société.

Pour des raisons de sécurité du réseau, est également considéré comme faisant partie du système d'information et de communication, le matériel personnel des salariés qui pourrait se connecter au réseau de l'entreprise, ou contenant des informations à caractère professionnel concernant l'entreprise.

1.2 utilisateurs concernés

Sauf mention contraire, la présente charte s'applique à l'ensemble des utilisateurs du système d'information et de communication de l'entreprise, quel que soit leur statut, à savoir tous les salariés, les intérimaires et stagiaires.

Les utilisateurs veillent à faire accepter les règles posées dans la présente charte à toute personne à laquelle ils permettraient d'accéder au système d'information et de communication, qu'il s'agisse d'employés de sociétés prestataires ou de visiteurs.

Chaque utilisateur a la responsabilité de protéger la confidentialité des e-Ressources de la Société.

2 Confidentialité des paramètres d'accès

L'accès à certains éléments du système d'information (comme la messagerie électronique ou téléphonique, les sessions sur les postes de travail, le réseau, certaines applications ou services interactifs) est protégé par des paramètres de connexion (identifiants et/ou mots de passe).

Ces paramètres sont personnels à l'utilisateur et doivent être gardés confidentiels. Ils permettent en particulier de contrôler l'activité des utilisateurs.

L'utilisateur ne doit pas s'approprier, modifier ou tenter de décrypter le mot de passe d'un autre utilisateur.

Dans la mesure du possible, ces paramètres doivent être mémorisés par l'utilisateur et ne pas être conservés, sous une forme permettant son accès aisé. En tout état de cause, ils ne doivent pas être transmis à des tiers.

Lorsqu'ils sont choisis par l'utilisateur, les paramètres doivent respecter un degré de complexité et être modifiés régulièrement. Il n'est pas autorisé que les mots de passe soient constitués de nom, prénom ou date. La composition de ces derniers est impérativement d'au moins 12 caractères avec majuscule, minuscule, chiffre et caractère spécial.

L'utilisateur ne doit pas utiliser de comptes autres que ceux auxquels il a légitimement accès.

Accès aux données

3.1 Sécurisation des accès

L'entreprise met en œuvre les moyens humains et techniques appropriés pour assurer la sécurité matérielle et logicielle du système d'information et de communication. A ce titre, il lui appartient de limiter les accès aux ressources sensibles et d'acquérir les droits de propriété intellectuelle ou d'obtenir les autorisations nécessaires à l'utilisation des ressources mises à disposition des utilisateurs.

Les personnes ayant accès à des données confidentielles du fait de leur activité sur la maintenance des e-ressources sont assujetties à une obligation de confidentialité sur les informations qu'ils sont amenés à connaître. L'entreprise s'engage à respecter les obligations légales en lien avec le règlement général de protection de la donnée.

En cas d'absence, même temporaire, il est impératif que l'utilisateur verrouille l'accès au matériel qui lui est confié.

A la fin de la journée, ils doivent sortir du système et mettre les équipements hors tension avant de s'absenter.

Il est strictement interdit de connecter un périphérique extérieur non validé par l'entreprise sur les équipements informatiques.

La connexion physique d'un téléphone sur les équipements, pour faire une recharge de sa batterie ou réaliser un transfert de données est interdit.

3.2 Utilisation du matériel

Il appartient à l'utilisateur de veiller à la sécurité du matériel utilisé et à son innocuité.

L'utilisateur s'engage à prendre soin du matériel et des locaux informatiques mis à sa disposition. Il informe immédiatement la direction et le prestataire informatique assurant la maintenance de toute anomalie constatée.

Le vol, la perte ou le détournement d'un ordinateur doivent être signalés dès que possible auprès du responsable des systèmes d'information monsieur …….. (Tél 06. . . .) le nom de l'utilisateur directement concerné, le modèle du matériel, la nature des informations contenues, la date du vol et les circonstances seront utiles au dépôt de plainte qui sera effectué auprès des services compétents.

L'utilisateur doit enregistrer les données sur les serveurs prévus à cet effet faisant partis des e-Ressources de l'entreprise.

Il est strictement interdit d'utiliser un périphérique de stockage personnel en le connectant sur un équipement informatique de la société. Cette interdiction concerne également la connexion physique d'un téléphone portable personnel.

L'utilisateur ne doit pas installer de logiciels, de copier ou d'installer des fichiers susceptibles de créer des risques d'atteinte à la sécurité au sein de l'Entreprise.

L'utilisateur veille au respect de la confidentialité des informations en sa possession. Il doit en toutes circonstances veiller au respect de la législation, qui protège notamment les droits de propriété intellectuelle, le secret des correspondances, les données personnelles, les systèmes de traitement automatisé de données, le droit à l'image des personnes, l'exposition des mineurs aux contenus préjudiciables.

Il ne doit en aucun cas se livrer à une activité concurrente à celle de l'entreprise ou susceptible de lui causer un quelconque préjudice en utilisant tout ou partie du système d'information et de communication.

L'utilisateur ne doit ni lire, ni copier, ni tenter de lire ou copier les fichiers d'un autre utilisateur sans son autorisation. Il ne doit également ni intercepter, ni tenter d'intercepter les communications privées entre utilisateurs, qu'elles consistent en courrier électronique ou en dialogue direct.

L'utilisateur n'est pas autorisé à télécharger et/ou installer de logiciel sur l'équipement informatique de l'entreprise. Seuls le personnel reconnu par sa fonction comme administrateur a cette possibilité après validation par la direction.

L'utilisateur doit veiller à l'utilisation professionnelle du matériel permettant une consommation raisonnable des ressources informatiques à disposition.

4 Utilisation d'internet

Dans le cadre de leur activité, les utilisateurs ont accès à internet. Pour des raisons de sécurité, l'accès à certains sites peut être limité ou interdit.

La Direction est habilitée à imposer des configurations du navigateur et à restreindre le téléchargement de certains fichiers.

La contribution des utilisateurs à des forums de discussion, systèmes de discussion instantanée, blogs, sites extérieurs à l'activité de l'Entreprise (tels que site communautaire), est interdite.

Les utilisateurs ne doivent en aucun cas se livrer à une activité illicite ou portant atteinte aux intérêts ou à l'image de l'Entreprise avec les moyens qu'elle met à leur disposition, y compris sur internet.

Seuls ont vocation à être consultés les sites internet présentant un lien direct et nécessaire à l'activité professionnelle au regard des fonctions exercées.

En particulier, l'utilisateur ne doit pas se connecter, sous peine de dénonciation aux instances judiciaires, sur des sites contraires à la législation en vigueur.

La transmission ou mise à disposition d'informations ou documents professionnels, par le biais d'internet ou de tout moyen de diffusion ou de stockage en ligne, est prohibée si elle ne sert pas directement l'activité professionnelle de l'utilisateur.

5 Messagerie

5.1 Mise à disposition

Chaque utilisateur dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique et d'un accès à la messagerie instantanée.

Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Les salariés doivent informer la direction des dysfonctionnements ou des doutes qu'ils constatent.

La transmission d'informations ou documents professionnels par courrier électronique ou messagerie instantanée à des fins ne servant pas directement l'activité professionnelle doit être limité et respecter des règles spécifiques (Cf chapitre 5.3).

5.2 Utilisation professionnelle

Avant tout envoi, il est impératif de vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises.

L'utilisateur doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs.

En cas d'envoi à une pluralité de destinataires, l'utilisateur doit respecter les dispositions relatives à la lutte contre l'envoi en masse de courriers non sollicités. Il doit également envisager l'opportunité de dissimuler certains destinataires, en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires.

En cas d'envoi à une liste de diffusion, il est important de vérifier la liste des abonnés à celle-ci.

Les utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques ne doivent comporter aucun élément illicite, tel que des propos diffamatoires, racistes, haineux, injurieux, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire.

5.3 Utilisation personnelle

Les messages à caractère personnel sont tolérés, à condition de respecter la législation en vigueur, de ne pas perturber et de respecter les principes posés dans la présente charte. Ils doivent être utilisés dans une quantité suffisamment raisonnable pour ne pas nuire à l'activité professionnelle de l'utilisateur ou celle des autres utilisateurs.

Les messages envoyés doivent être signalés par la mention « Privé » dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé « Privé ».

Les messages reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé «Privé».

En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel et peuvent faire l'objet d'une lecture par la direction où le service informatique de l'entreprise.

6 Contrôle des activités

6.1 Contrôles automatisés

Le système d'information et de communication s'appuie sur des fichiers journaux (« logs »), créés en grande partie automatiquement par les équipements informatiques et de télécommunication. Ces fichiers sont stockés sur les postes informatiques et sur le réseau. Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations de l'entreprise, en détectant des erreurs matérielles ou logicielles et en contrôlant les accès et l'activité des utilisateurs et des tiers accédant au système d'information.

Les utilisateurs sont informés que des traitements sont réalisés afin de surveiller l'activité du système d'information et de communication de l'entreprise.

L'attention des utilisateurs est attirée sur le fait qu'il est ainsi possible de contrôler leur activité et leurs échanges. Des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements, dans le respect des règles en vigueur.

6.2 Contrôles manuels

En cas de dysfonctionnement, il peut être procédé à un contrôle manuel et à une vérification de toute opération effectuée par un ou plusieurs utilisateurs.

Lorsque le contrôle porte sur les fichiers d'un utilisateur, et sauf risque ou événement particulier, les fichiers identifiés par le salarié comme personnels, sauvegardés dans un répertoire dénommé « privé », ne peuvent être consultés.

7 Sanctions

Le manquement aux règles et mesures de sécurité de la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés.

Dès lors qu'une sanction disciplinaire est susceptible d'être prononcée à l'encontre d'un utilisateur, celui-ci est informé dans un bref délai des faits qui lui sont reprochés, sauf risque ou événement particulier.

En fonction du non-respect de la présente charte, des agissements peuvent également entraîner des poursuites pénales que l'utilisateur auteur des faits devra assumer devant la juridiction concernée.

8 Information des salariés

La présente charte est communiquée individuellement à chaque salarié.

9 Entrée en vigueur

La présente charte est applicable à compter du …….

Pris connaissance le

Nom : prénom : Signature :