CHARTE D'UTILISATION

DES RESSOURCES INFORMATIQUES

DE MISTRAL HABITAT

MISTRAL habitat

SOMMAIRE

1 – PREAMBULE

1.1 – Objet de la charte

Cette charte a pour vocation d'exposer les droits et obligations de chacun et de fixer les règles et précautions que tout utilisateur doit respecter et mettre en œuvre dans l'utilisation des ressources informatiques de l'entreprise.

La présente charte intègre la règlementation en vigueur depuis le 25 mai 2018 en matière de protection des données à caractère personnel exigée par le règlement européen 2016/679 du 27 avril 2016 dit « RGPD ».

L'entreprise doit, pour des raisons légales et déontologiques, garantir la sécurité des ressources informatiques qu'elle détient en assurant, en interne et vis à vis des tiers, la confidentialité, la disponibilité, la pérennité et l'intégrité des informations stockées dans ses fichiers et bases de données.
Elle doit également s'assurer que ses ressources informatiques sont utilisées à bon escient, conformément à la loi et aux usages.

Les ressources informatiques de l'entreprise sont sa propriété.

Les informations et les ressources informatiques de l'entreprise peuvent être confidentielles ou sensibles pour l'entreprise ou pour des tiers. Les utilisateurs doivent protéger les informations de l'entreprise et celles qui appartiennent à des tiers, tels que clients, partenaires et fournisseurs, contre la divulgation non autorisée, la modification, les dommages ou la destruction. Il appartient à chaque utilisateur de gérer, d'entretenir et de protéger correctement la sécurité des ressources informatiques de l'entreprise auxquelles il a accès ou qu'il contrôle.

1.2 – Définitions

Par « l'entreprise », on désigne le propriétaire des ressources informatiques mises à la disposition des utilisateurs.

Par "ressources informatiques", il faut entendre l'ensemble des dispositifs informatiques mis à la disposition des utilisateurs tels que : ordinateurs, logiciels, applications, bases de données, moyens et réseaux de télécommunication, courrier électronique, Internet, Intranet, Extranet ainsi que les fichiers, bases de données et informations qu'ils contiennent. Les équipements nomades, tels que les ordinateurs portables, téléphones portables, tablettes, supports amovibles (clefs USB…) sont également des ressources informatiques.

Dans le cadre de l'utilisation des ressources informatiques, il convient de distinguer trois catégories d'acteurs :

1. Le terme d' « utilisateur » recouvre tout personnel ayant un accès autorisé aux ressources informatiques de l'entreprise quel que soit son statut. Il s'agit notamment des membres du personnel de l'entreprise travaillant au sein de la société (salariés, fonctionnaires, stagiaires, intérimaires etc.), des administrateurs, ou du personnel extérieur (sous-traitants, prestataires etc.).

2. Le terme d' « Administrateurs système » désigne le personnel responsable techniquement du bon fonctionnement des ressources informatiques.

3. Le « Responsable des Systèmes d'Information » supervise et encadre le travail des Administrateurs système et applique la politique de sécurité informatique définie avec la Direction Générale.

1.3 – Champ d'application

Les règles d'usage et de sécurité figurant dans la présente charte s'appliquent à l'entreprise ainsi qu'à l'ensemble des utilisateurs.

2 – CONDITIONS D'UTILISATION DES RESSOURCES INFORMATIQUES

2.1 - Utilisation professionnelle / privée

Les ressources informatiques sont des outils de travail ouverts à des usages professionnels légitimes et en conformité avec les dispositions de la présente charte.
Elles peuvent également constituer le support d'une communication privée limitée, dans les conditions décrites ci dessous.

L'utilisation résiduelle des ressources informatiques à titre privé doit être non lucrative et raisonnable, tant dans sa fréquence que dans sa durée. Cette utilisation ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service, et doit respecter les dispositions, notamment de sécurité, de la présente charte.

Toute information est réputée professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée.
Il appartient à l'utilisateur d'identifier les fichiers et messages qui sont personnels (dans l'objet du message ou dans le nom du fichier).
À défaut d'une telle identification, les fichiers et messages sont présumés être professionnels, de sorte que l'employeur peut y accéder librement.

L'utilisation des ressources informatiques à titre privé doit respecter la réglementation en vigueur. En particulier, la consultation, détention, diffusion et exportation d'images ou contenus à caractère pédophile, pornographique, raciste ou antisémite est totalement interdite.

2.2 - Continuité de service : gestion des absences et des départs

Aux seules fins d'assurer la continuité de service, l'utilisateur informe sa hiérarchie des modalités permettant l'accès aux ressources mises spécifiquement à sa disposition.

La diffusion d'un message automatique d'absence par courrier électronique est nécessaire en cas d'absence supérieure à trois jours.

Lors de son départ définitif de l'entreprise, l'utilisateur est tenu de restituer les téléphones, tablettes et autres outils de communication, qui lui auront été confiés en vue de l'exécution de son travail, et ce, en bon état.

Le Responsable des Systèmes d'Information avertira l'utilisateur qui quitte l'entreprise de la date de fermeture de son compte, afin de lui permettre de vider sa messagerie. L'adresse électronique nominative de l'utilisateur sera ensuite supprimée, après son départ effectif.

Il appartiendra à l'utilisateur, dans la mesure du possible, d'informer par message électronique les membres du personnel ainsi que ses interlocuteurs externes de son départ définitif de l'entreprise, en précisant le nom du ou des nouveaux destinataires/interlocuteurs, afin d'assurer la continuité du service et des échanges professionnels.

2.3 – Accès à distance

Dans le cadre de l'évolution des conditions de travail, des services d'accès à distance à la messagerie ou à d'autres ressources informatiques sont mis en place.
L'utilisateur peut être autorisé à utiliser son matériel personnel pour accéder à distance aux Systèmes d'Information, depuis un lieu autre que son lieu de travail, et se connecter à certaines ressources spécifiques.
L'accès est soumis à l'autorisation expresse du Responsable des Systèmes d'Information.
L'ensemble des règles décrites dans la charte concernant l'utilisation des ressources restent applicables. Dans les cas d'utilisation des services d'accès à distance, afin de limiter le risque de divulgation d'information, des précautions particulières s'imposent :

- Etre particulièrement vigilant afin de ne pas divulguer d'information confidentielle lors d'une consultation à distance (Regard indiscret d'un tiers, etc.).
- Se déconnecter systématiquement et complètement du service d'accès à distance après utilisation.

3 – REGLES GENERALES DE SECURITE

Les niveaux d'accès ouverts à l'utilisateur sont définis en fonction de la mission qui lui est conférée.

Afin d'assurer la sécurité des ressources informatiques de l'entreprise et dans le cadre de la règlementation relative à la protection des données, sont notamment interdites les actions suivantes ou les tentatives de les réaliser :

- Interrompre ou perturber le fonctionnement normal des ressources informatiques (manipulations anormales, introduction de virus ou autres dispositifs nuisibles, chargement de données non contrôlées, etc.).
- Se connecter ou essayer de se connecter sur un site extérieur à l'établissement sans y être expressément autorisé.
- Accéder au compte ou aux informations d'un autre utilisateur sans y être expressément autorisé.
- Modifier ou détruire des informations appartenant à d'autres utilisateurs sans leur autorisation expresse.
- accéder ou supprimer des informations si cela ne relève pas des tâches habituelles incombant à l'utilisateur.
- Porter atteinte à l'intégrité d'un autre utilisateur ou à sa sensibilité, notamment par l'intermédiaire de messages, images ou textes provocants.
- Masquer sa véritable identité, en particulier en se connectant sous le nom d'un autre utilisateur.
- Confier ses identifiants et mot de passe à un tiers.
- Développer, copier, modifier, détruire, charger et/ou installer des logiciels ou matériels sans l'autorisation expresse du Responsable des Systèmes d'Information.
- Connecter des supports amovibles tels qu'une clef USB sans l'autorisation expresse du Responsable des Systèmes d'Information.
- Nuire à l'image de marque de l'entreprise par une mauvaise utilisation des ressources informatiques.

- Envoyer ou recevoir, par le biais des ressources informatiques de l'entreprise, des éléments protégés par des droits de reproduction, de secrets commerciaux, d'informations confidentielles, exclusives ou financières ou d'éléments similaires sans autorisation appropriée.
- Divulguer des informations confidentielles sur des membres du personnel, l'entreprise ou ses clients.

Sont également imposées à l'utilisateur les obligations suivantes :

- Verrouiller son ordinateur dès que l'on quitte son poste de travail.
- Signaler aux Administrateurs système ou au Responsable des Systèmes d'Information, dans les meilleurs délais, toute violation ou tentative de violation suspectée ou constatée de son compte informatique et de manière générale tout dysfonctionnement ou anomalie.
- respecter les procédures préalablement définies par l'entreprise afin d'encadrer les opérations de copie de données sur des supports amovibles, notamment en obtenant l'accord préalable du supérieur hiérarchique ou du Responsable des Systèmes d'information et en respectant les règles de sécurité.
- Signaler au Responsable des Systèmes d'Information toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation.

4 - COMPTES, IDENTIFIANTS ET MOTS DE PASSE

Les comptes, les identifiants et les mots de passe utilisés pour accéder aux ressources informatiques sont des informations personnelles délivrées individuellement à chaque utilisateur ou mis en place par ce dernier.

L'association d'un identifiant spécifique et d'un mot de passe constitue une clé logique unique qui :

- utilisée correctement, réduit notablement les risques d'accès non autorisés aux ressources informatiques,
- identifie un utilisateur unique, et le désigne comme seul auteur possible des création, modification ou suppression d'enregistrements dans les bases de données de l'entreprise, dans les applications gérant une traçabilité liée à l'identifiant.

Les mots de passe doivent être conservés de façon strictement confidentielle.

Ils doivent être construits suivants des règles précisées par le service des Systèmes d'Information et imposant un niveau de complexité renforçant leur inviolabilité (combinaison de lettres, chiffres et caractères spéciaux). Ils doivent être renouvelés régulièrement.

Une stratégie de contrôle est mise en place par le Responsable des Systèmes d'Information, interdisant la création et l'utilisation de tout mot de passe n'obéissant pas à ces règles. De même, cette stratégie impose aux utilisateurs le renouvellement de leur mot de passe à échéances régulières.

L'utilisateur ne doit communiquer ses comptes et mots de passe ou permettre l'utilisation des ressources informatiques de l'entreprise auxquelles il a accès, même de manière temporaire, à d'autres utilisateurs internes et externes à l'entreprise.

Toutefois, si un membre du personnel absent détient sur son poste des informations indispensables à la poursuite de l'activité, l'employeur peut exiger la communication de ses codes si le Responsable des Systèmes d'Information n'est pas en mesure de fournir l'accès au poste.

L'utilisateur doit s'identifier clairement lorsqu'il se connecte à des ressources informatiques nécessitant une identification préalable : il est strictement interdit d'usurper l'identité d'autrui ou d'agir de façon anonyme.

En cas de violation ou de simple tentative de violation de son compte, l'utilisateur doit immédiatement prévenir les Administrateurs système ou le Responsable des Systèmes d'Information.

5 - SECURITE DU POSTE DE TRAVAIL

Il est obligatoire de verrouiller son ordinateur dès que l'on s'absente de son poste de travail.

Par ailleurs, l'utilisateur doit sortir du système et mettre son ordinateur hors tension avant de quitter son lieu de travail. Cette disposition est également souhaitable pour une absence prolongée en cours de journée.

Si un système informatique présente des anomalies, les Administrateurs système doivent en être informés immédiatement. Une anomalie peut être l'indice d'une infection par un virus ou d'un autre problème de sécurité.

Le vol ou le détournement d'un ordinateur, notamment un portable, ou de tout support informatique (tablette, support amovible etc.), doit être signalé aussi rapidement que possible au supérieur hiérarchique et au Responsable des Systèmes d'Information, en fournissant le nom de l'utilisateur directement concerné, la nature des informations contenues sur le disque dur ou le support, la date du vol ou de la disparition, ainsi que toutes autres informations pertinentes relatives au vol ou à la disparition.

L'utilisateur doit respecter les procédures préalablement définies par l'entreprise afin d'encadrer les opérations de copie de données sur des supports amovibles, notamment en obtenant l'accord préalable du supérieur hiérarchique et en respectant les règles de sécurité.

L'utilisateur ne doit pas modifier les configurations matérielles et logicielles propriétés de l'entreprise sans autorisation expresse du Responsable des Systèmes d'Information.

Sur les sites (siège, agence...), le raccordement des matériels aux réseaux de communication internes et externes est géré par le Responsable des Systèmes d'Information. Ces raccordements ne peuvent être modifiés qu'avec son autorisation expresse préalable.

La connexion d'une machine personnelle au réseau local sans autorisation expresse du Responsable des Systèmes d'Information est strictement interdite.

6 - UTILISATION D'INTERNET ET DES COURRIERS ELECTRONIQUES

6.1 - Internet

Il est rappelé qu'Internet est soumis à l'ensemble des règles de droit en vigueur. L'utilisation d'Internet (et par extension intranet et extranet) constitue l'un des éléments essentiels d'optimisation du travail et d'accessibilité de l'information au sein et en dehors de l'entreprise.

Un accès Internet est fourni à chaque utilisateur au travers de son identification sur le réseau. Cette identification permet de tracer l'utilisation qui est faite d'internet par chaque Utilisateur.

L'utilisateur doit faire usage des services Internet dans le cadre légitime de ses activités professionnelles et dans le respect de principes généraux et de règles propres aux divers sites sur lesquels il se connecte ainsi que dans le respect de la législation en vigueur.
Si une utilisation résiduelle privée, telle que définie à l'article 2.1, peut être tolérée, il est rappelé que les connexions établies grâce à l'outil informatique mis à disposition par l'entreprise sont présumées avoir un caractère professionnel. L'entreprise peut les rechercher aux fins de les identifier et de les exploiter si nécessaire (cf article 10 – Contrôles et mesures de sécurité).

En complément des règles générales listées à l'article 3, l'utilisation d'Internet nécessite notamment un strict respect des dispositions suivantes :

- L'utilisateur ne doit pas se connecter ou essayer de se connecter sur un serveur autrement que par les dispositions prévues par l'entreprise et par ce serveur.
- Il ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède et/ou des ressources informatiques de l'entreprise.
- Il ne doit pas usurper l'identité d'une autre personne et il ne doit pas intercepter de communications entre tiers.
- Il 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.
- Il ne doit pas déposer de documents sur un serveur sauf si celui-ci le permet ou sans y être autorisé par les responsables habilités.
- Il doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques par courrier, forums de discussions, « chat » (espace de dialogue en temps réel), etc.
- Il ne doit pas émettre d'opinions personnelles étrangères à son activité professionnelle susceptibles de porter préjudice à l'entreprise.
- Il doit s'imposer les règles de bon usage et le respect des lois : il est notamment interdit de se connecter sur des sites ou d'échanger des informations à caractère injurieux, raciste, discriminatoire, pédophile, pornographique ou diffamatoire. Les messages à caractère commercial et le prosélytisme sont également interdits.
- Il ne doit pas envoyer du courrier en chaîne, participer à des jeux en ligne, télécharger des jeux, des économiseurs d'écran, de la musique, des logiciels et (sauf nécessité professionnelle) s'inscrire à des listes de diffusion, ou des groupes de discussion, ou envoyer des messages à des groupes d'échange.
- L'utilisateur qui reçoit des éléments non autorisés ou constituant une violation de lois et règles internes doit en aviser immédiatement le Responsable des Systèmes d'Information.

- L'utilisateur sollicitera l'assistance des Administrateurs système pour l'ouverture de courriers électroniques avec ou sans pièces jointes, qui ne lui sont pas clairement destinés, susceptibles de contenir des virus ou autres dispositifs nuisibles.
- L'utilisateur ne doit pas envoyer par courrier électronique, déposer par messagerie vocale, télécharger ou transmettre par Internet une information confidentielle sauf si ces envois sont réalisés dans le cadre professionnel et à l'aide d'une application sécurisée utilisant une méthode de chiffrement, en accord avec le Responsable des Systèmes d'Information.

En effet d'une part, la navigation sur Internet met en œuvre des réseaux de communication mondiaux et des processus qui échappent au contrôle individuel des internautes et qui sont susceptibles de conserver des traces des sites visités ainsi que des échanges d'informations réalisés. Ces traces peuvent être utilisées à des fins commerciales ou de surveillance.

D'autre part, le courrier électronique et les autres informations communiquées par Internet peuvent être interceptés ou modifiés subrepticement durant la transmission.

6.2 – Courriers électroniques

Chaque Utilisateur dispose d'une boîte aux lettres électronique professionnelle nominative lui permettant d'émettre et de recevoir des messages électroniques.

L'aspect nominatif de l'adresse électronique constitue le simple prolongement de l'adresse de l'entreprise : il ne retire en rien le caractère professionnel de la messagerie.

Une adresse électronique, fonctionnelle ou organisationnelle, peut être mise en place pour un utilisateur ou un groupe d'utilisateurs pour les besoins de l'entreprise.

Ces listes de diffusion, désignant une catégorie ou un groupe d'utilisateurs, ne peuvent être créées ou utilisées sans autorisation expresse du Responsable des Systèmes d'Information.

L'utilisateur est informé qu'un message électronique peut constituer une preuve susceptible d'engager sa responsabilité.
Il doit, en conséquence, être vigilant sur la nature des messages électroniques qu'il échange et s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages. Il doit également organiser et mettre en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve.

L'usage des adresses électroniques et de la messagerie dans son ensemble ne peuvent viser des fins commerciales, politiques ou idéologiques. La communication des adresses à des tiers par le propriétaire ou l'usage de la messagerie qu'ils pourraient en faire n'engagent pas la responsabilité de l'entreprise.

Tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son caractère privé (objet du message ou nom du répertoire).

En raison notamment de son identification véhiculant l'image de marque de l'entreprise et engageant sa responsabilité au même titre qu'un papier à en-tête ou un tampon, en ce qui concerne l'utilisation des adresses électroniques et de la messagerie à des fins privées, seules les communications « de particulier à particulier », entre deux personnes

agissant à titre personnel en dehors de tout cadre commercial, seront tolérées, dans les conditions suivantes :

- Le destinataire du message doit être une personne physique identifiée et connue de l'émetteur. Les communications à destination d'adresses génériques de personnes morales sont notamment interdites.
- La communication électronique ne peut en aucun cas avoir pour objet de préparer, de réaliser ou d'effectuer le suivi d'opérations commerciales, juridiques ou financières quelles qu'elles soient.

Sont interdits les messages comportant des contenus à caractère illicite quelle qu'en soit la nature. Il s'agit notamment des contenus contraires aux dispositions de la loi sur la liberté d'expression ou portant atteinte à la vie privée d'autrui et les contenus caractère pédophile, pornographique, raciste ou antisémite etc.

Un guide des bonnes pratiques relatif à la gestion de la messagerie électronique est disponible dans l'Intranet.

7 – DROIT A LA DECONNEXION

Le droit à la déconnexion, entré en vigueur le 1er janvier 2017 dans le cadre de la loi travail du 8 août 2016, s'entend comme le droit de chaque salarié de ne pas répondre aux courriels et autres messages en dehors des heures de travail, afin de garantir l'équilibre entre vie professionnelle et vie privée, les temps de repos et de récupération.

Les modalités d'exercice du droit à la déconnexion dans l'entreprise figure dans l'accord d'entreprise sur l'égalité professionnelle entre les femmes et les hommes, consultable sur le site Intranet de l'entreprise.

8 - RESPECT DE LA PROPRIETE

L'entreprise rappelle que l'utilisation des ressources informatiques implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et plus généralement, de tous tiers titulaires de tels droits.

En conséquence, chaque utilisateur doit :

- Utiliser les logiciels dans les conditions des licences souscrites,
- Ne pas contourner ou tenter de contourner les restrictions d'utilisation d'un logiciel,
- Ne pas reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

9 - PROTECTION DES DONNEES PERSONNELLES

L'utilisateur est informé de la nécessité de respecter les dispositions légales en matière de traitement, automatisé ou non, de données à caractère personnel, conformément à la loi « informatique et libertés » et au « RGPD ».

La loi n°78-17 du 6 janvier 1978 modifiée en 2004 relative à l'informatique, aux fichiers et aux libertés, dite « loi informatique et libertés » énonce que : « le responsable du traitement est tenu de prendre toutes les précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès » (article 34).

Le règlement européen 2016/679 du 27 avril 2016 sur la protection des données à caractère personnel, dit « RGPD », renforce la loi informatique et libertés et précise que la protection des données personnelles nécessite de prendre des « mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque » (article 32).

En cas de manquement, le responsable de traitement encoure une amende allant jusqu'à dix millions d'euros (10 M€), voire jusqu'à 2% de son chiffre d'affaires annuel mondial (RGPD, article 83, §4).

Les données à caractère personnel sont des informations qui permettent – sous quelque forme que ce soit – directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent (par exemple : nom, coordonnées, adresse IP...).

Un traitement est une opération ou un ensemble d'opérations effectuées ou non à l'aide de procédés informatisés ou automatisés et appliqués à des données ou des ensembles de données (par exemple : collecte, enregistrement, modification, extraction, consultation, utilisation, communication par transmission, diffusion, effacement, etc.).

Le RGPD définit les conditions dans lesquelles des traitements de données à caractère personnel peuvent être effectués. Il consacre les droits d'accès, de rectification et d'opposition à un traitement de leurs données personnelles des personnes concernées et leur ouvre un droit à l'effacement (droit à l'oubli), un droit à la limitation du traitement ainsi qu'un droit à la portabilité de leurs données, y compris les données portant sur l'utilisation des ressources informatiques.

Ces droits s'exercent auprès du délégué à la protection des données.

Le délégué à la protection des données veille en outre au respect de la législation en matière de protection des données. Il veille au respect des droits des personnes concernées, à mettre en place et maintenir un niveau de sécurité adapté aux risques et à notifier toute violation de données auprès de la CNIL.

10 – RESPONSABILITES

La sécurité est notre priorité : chaque utilisateur des ressources informatiques doit y contribuer à son niveau et mettre en application les règles et recommandations fournies dans la présente charte. Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques mises à sa disposition.

Il convient également de préciser que le non-respect de certaines règles peut contrevenir aux lois françaises et engager la responsabilité de son auteur, en particulier dans le domaine de la sécurité informatique :

- Loi du 6 janvier 1978 dite « informatique et libertés », renforcée par le règlement européen 2016/679/UE du 27 avril 2016 relatif à la protection des personnes

physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données dit « RGPD »).

- Loi du 5 janvier 1988 relative à la fraude informatique, dite « loi Godfrain », reprise dans les articles 323-1 à 323-7 du code pénal, réprimant les actes de criminalité informatique et de piratage (atteintes aux systèmes de traitement automatisé de données).
- La législation relative à la propriété intellectuelle et plus particulièrement les lois du 3 juillet 1985 et du 1er juillet 1992 sur la protection des logiciels. Ces lois qui protègent les droits d'auteur, interdisent en particulier à l'utilisateur d'un logiciel toute reproduction autre que l'établissement d'une copie de sauvegarde.
- La Loi du 10 mai 1994, transposant au droit français la directive du Conseil des Communautés Européennes du 14 mai 1991 concernant la protection juridique des programmes d'ordinateurs, et la Loi du 5 février 1994 relative à la répression de la contrefaçon.
- L'article 227-23 du code pénal, qui criminalise le fait de fixer, d'enregistrer ou de transmettre, en vue de sa diffusion, l'image ou la représentation d'un mineur qui présente un caractère pornographique.

Et autres dispositions pénales concernant le secret des correspondances, les droits de l'enfant, la lutte contre le racisme et la discrimination, etc.

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

Le texte complet de ces lois peut être consulté auprès de la Direction des Ressources Humaines.

11 – CONTROLES ET MESURES DE SECURITE

11.1 – Mesures de sécurité

Les Administrateurs système et le Responsable des Systèmes d'Information sont amenés, dans le cadre normal de leur travail, à réaliser les tâches suivantes :

- Configurer et administrer les ressources informatiques dans le sens d'une meilleure sécurité et dans l'intérêt des utilisateurs.
- Accéder, sur les ressources qu'ils administrent, aux informations privatives à des fins de diagnostic et d'administration, en respectant scrupuleusement la confidentialité de ces informations et en s'efforçant, tant que la situation ne l'exige pas, de ne pas les altérer.
- Etablir des procédures de surveillance de toutes les tâches exécutées sur les ressources informatiques et/ou installer des matériels ou des logiciels spécifiques, afin de déceler les violations ou les tentatives de violation des dispositifs de sécurité.
- Prendre des mesures conservatoires si l'urgence l'impose, sans préjuger des sanctions résultantes des infractions à la présente charte.

Les Administrateurs système, dans le cadre de leur activité professionnelle au sein de L'entreprise, sont tenus :

- D'informer préalablement le Responsable des Systèmes d'Information de toute mise en œuvre de procédures exceptionnelles de surveillance ou d'investigation.

- D'informer immédiatement le Responsable des Systèmes d'Information de tout comportement d'un utilisateur contraire aux dispositions de cette charte.
- De coopérer avec les correspondants sécurité des réseaux extérieurs en cas d'incident de sécurité impliquant une machine qu'ils administrent.

Le Responsable des Systèmes d'Information, dans le cadre de son activité professionnelle au sein de L'entreprise, est tenu :

- De veiller à ce que les ressources sensibles ne soient accessibles qu'aux personnes habilitées, en dehors des mesures d'organisation de la continuité du service mises en place par la hiérarchie.
- De limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité.
- D'interdire temporairement ou définitivement à des fins conservatoires l'accès à tout ou partie des ressources informatiques à un utilisateur qui ne respecte pas la présente charte, sans préjuger des éventuelles poursuites ou procédures de sanctions en découlant.
- De saisir l'autorité hiérarchique des manquements graves résultant du non-respect de cette charte pouvant déclencher des procédures disciplinaires ou pénales.
- De soutenir de son autorité les Administrateurs système dans leur travail de mise en application de la présente charte.

L'utilisation des ressources informatiques de l'entreprise sous-entend l'acceptation implicite par l'utilisateur de l'administration de son poste de travail par les Administrateurs système, sans restriction.

L'utilisateur est informé :

- que pour effectuer la maintenance corrective, curative ou évolutive, le Responsable des Systèmes d'Information se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition ;
- qu'une maintenance à distance est précédée, dans la mesure du possible, d'une information de l'utilisateur ;
- que toute information bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire, sera isolée ; le cas échéant supprimée.

11.2 – Surveillance et contrôles

L'entreprise informe l'utilisateur que l'utilisation des ressources informatiques donne lieu à une surveillance, un contrôle et une analyse à des fins statistiques, de traçabilité réglementaire ou fonctionnelle, d'optimisation, de sécurité ou de détection des abus, dans le respect de la législation applicable.
L'entreprise pourra exploiter ces informations, qui sont conservées pendant une durée n'excédant pas celle prévue par la législation en vigueur, pour vérifier que l'utilisation des ressources informatiques est conforme aux dispositions de cette charte, ou à l'occasion d'une procédure judiciaire.

A cet effet, via des dispositifs tels que le firewall (ou pare-feu), la sonde de détection d'intrusion ou le proxy (filtrage des requêtes des utilisateurs et contrôle des accès), est mis en place un système de journalisation des accès Internet (conservation des informations techniques de connexion telles que l'heure et la durée d'accès, l'adresse IP de l'utilisateur, l'historique de navigation...), de la messagerie et des données échangées,

permettant de procéder au contrôle a posteriori des sites visités par chaque utilisateur et de l'utilisation faite des ressources informatiques mises à leur disposition.

D'autre part, afin de prévenir l'accès à certains sites non autorisés en raison de leur caractère immoral, illicite, illégal (pornographie, pédophilie, racisme, incitation à la haine, etc.), un dispositif de filtrage et de contrôle a été mis en œuvre.

L'entreprise se réserve également le droit d'interdire l'accès à certains sites Internet sans utilité professionnelle ou certaines ressources informatiques sans qu'il soit nécessaire d'en aviser préalablement les utilisateurs. Ce filtrage peut être différent selon la fonction de l'agent.

Le Responsable des Systèmes d'Information pourra faire auditer à tout moment le contenu des dispositifs de stockage mis à la disposition de l'utilisateur, y compris sur son poste de travail individuel, pour vérifier que les dispositions de la présente charte sont bien respectées.

Le personnel du service informatique respecte la confidentialité des données et des traces auxquelles il est amené à accéder dans l'exercice de ses fonctions, mais peut être amené à les utiliser pour mettre en évidence certaines infractions commises par les utilisateurs.

12 – SANCTIONS

Le non-respect des règles et mesures de sécurité figurant dans la présente charte peut constituer une faute grave, et engage la responsabilité personnelle de l'utilisateur dès lors qu'il est prouvé que les faits fautifs lui sont personnellement imputables et l'expose éventuellement et de manière appropriée et proportionnée au manquement commis, à des sanctions disciplinaires.

Si l'entreprise constate une faute, notamment une violation de la présente charte ou de toute autre procédure, directive ou instruction de l'entreprise ou un acte criminel impliquant des ressources informatiques de l'entreprise, les fichiers ou informations contenus dans celles-ci pourront être utilisés pour documenter cette faute et pourront être divulgués aux autorités compétentes, à l'intérieur et à l'extérieur de l'entreprise, et l'utilisateur sera passible d'une sanction disciplinaire et de poursuites judiciaires auprès du Tribunal compétent.

13 – ENTREE EN VIGUEUR

Les règles définies dans la présente charte ont été fixées par la Direction de l'entreprise dans le respect des dispositions législatives et règlementaires applicables et soumises à la consultation du Comité d'Entreprise.

La présente charte se substitue, à compter de sa signature, à la charte signée le 24 juin 2002 précédemment en vigueur.

Fait à Avignon, le 1er octobre 2018.

Le Directeur Général de MISTRAL habitat

Le Directeur Général,

Philippe BRUNET-DEBAINES