CHARTE D'UTILISATION DES MOYENS INFORMATIQUES ET DE COMMUNICATION ELECTRONIQUE

ANNEXE AU REGLEMENT INTERIEUR

Sommaire

1. Contexte et objet

Le présent document est rédigé dans l'intérêt de chacun des utilisateurs du système d'information d'**ASSURMER** avec pour objectifs de :

- Respecter les lois et règlementations en vigueur
- Assurer un développement harmonieux des accès au SI pour les utilisateurs
- Définir et mettre en œuvre les moyens appropriés, selon l'état de l'art de la technique, pour protéger les utilisateurs et les moyens informatiques mis à leur disposition contre les risques de destruction, d'altération, de fraude ou encore de vol.

ASSURMER est seule habilitée à l'ouverture et au maintien des accès à son système d'information. Il fournit notamment à ses collaborateurs et à ses prestataires des moyens informatiques destinés à une utilisation professionnelle.

En vue de maintenir un environnement de travail professionnel et de protéger les informations confidentielles qui sont la propriété d'ASSURMER, de ses clients ou encore de ses partenaires, chaque utilisateur est tenu au respect des règles et bonnes pratiques mentionnées dans le présent document.

Le présent document a pour objet de préciser les droits et devoirs des utilisateurs des système d'information. Il est conforme aux dispositions légales et règlementaires en vigueur. Il définit notamment les règles d'utilisation et d'accès :

- Au système d'information
- Aux services Internet
- Aux ordinateurs fixes, portables, serveurs
- Au courrier électronique et autres outils d'échanges d'information
- Aux services intranet et extranet
- A la téléphonie

Et de manière générale à l'ensemble de l'infrastructure et des moyens informatiques.

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 connecté au réseau de l'entreprise, ou contenant des informations à caractère professionnel concernant l'entreprise.

Il est à noter que le présent document constitue une annexe au règlement intérieur.

2. Champ d'application

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, y compris les mandataires sociaux, salariés, intérimaires, stagiaires, employés de sociétés prestataires, visiteurs occasionnels. Les salariés veillent à faire accepter valablement les règles posées dans la présente charte à toute personne à laquelle ils permettraient, dans la stricte limite de leurs droits, d'accéder au système d'information et de communication.

3. 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, mots de passe).

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

Dans la mesure du possible, ces paramètres doivent être mémorisés par l'utilisateur et ne pas être conservés, sous quelque forme que ce soit. En tout état de cause, ils ne doivent pas être transmis à des tiers ou aisément accessibles. Ils doivent être saisis par l'utilisateur à chaque accès et ne pas être conservés en mémoire dans le système d'information.

L'utilisateur ne doit pas usurper, emprunter ou encore tenter d'obtenir l'identifiant et mot de passe d'autres utilisateurs.

Lorsqu'ils sont choisis par l'utilisateur, les paramètres doivent respecter un certain degré de complexité et être modifiés régulièrement. Des consignes de sécurité sont fixées par la politique de sécurité afin de recommander les bonnes pratiques en la matière.

4. Protection des ressources sous la responsabilité de l'utilisateur

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. À 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 "utilisation des ressources mises à disposition des utilisateurs.

Le Responsable du Système d'Information (RSI) est responsable du contrôle du bon fonctionnement du système d'information et de communication. Il veille à l'application des règles de la présente charte, en concertation avec le Service des Ressources Humaines. Les membres de l'équipe informatique (Responsables du système d'information, le comité Informatique, et le/les prestataire(s)intervenant sur le sujet) sont assujettis à une obligation de confidentialité sur les informations qu'ils sont amenés à connaître.

L'utilisateur est responsable quant à lui des ressources qui lui sont confiées dans le cadre de l'exercice de ses fonctions. Il doit concourir à la protection des dites ressources, en faisant preuve de prudence notamment à l'extérieur des locaux d'ASSURMER. En cas d'absence, il est impératif que l'utilisateur verrouille l'accès au matériel qui lui est confié ou à son propre matériel, dès lors que celui-ci contient des informations à caractère professionnel.

En suivant les règles de cette charte et en utilisant les outils informatiques exclusivement de la façon proposée et demandée par ASSURMER, l'utilisateur est généralement en respect des droits donnés à l'utilisateur. Cependant, s'ajoutent des principes de précaution et de bon sens. En cas de doute, sur l'ouverture d'un mail, d'un fichier, d'une application, il est recommandé de contacter le RSI au préalable.

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 le système d'information et de communication.

Si l'utilisateur dispose d'un ordinateur portable, il doit effectuer des sauvegardes régulières sur le réseau d'ASSURMER.

L'utilisateur n'est pas autorisé à :

Installer des logiciels autres que ceux proposés par Microsoft 365 sur son matériel informatique. Il appartient au responsable du Système d'Information de décider sur demande écrite faite par mail si un logiciel supplémentaire peut être installé sur le matériel informatique ;

Copier ou installer des fichiers susceptibles de créer des risques de sécurité au sein de l'entreprise. Il doit dans tous les cas en alerter l'équipe informatique.

L'utilisation des supports amovibles (clé USB, disque dur externe ...) est limitée à un certain groupe d'employés définis par ASSURMER pour des besoins liés à leurs activités professionnelles.

Ce même groupe est seulement autorisé à utiliser un support de stockage virtuel. Pour les autres utilisateurs non visés l'utilisation de tels moyens de stockage n'est pas autorisée. Il est de la responsabilité de l'utilisateur de ces supports de s'interroger, avant toute utilisation sur le risque potentiel, notamment de virus informatique, provenant d'un tel matériel. En cas de doute, l'utilisateur doit contacter le Responsable du Système d'Information.

Lorsque les supports amovibles sont utilisés à des fins de sauvegarde, leur stockage doit être sécurisé. L'utilisateur est responsable de ceux-ci notamment en cas de vol, perte ou altération. Le RSI propose à ces utilisateurs des clefs USB sécurisées.

Toutes entrées et sorties de données via une clef USB, un disque dur externe, des moyens de stockage virtuel etc...seront enregistrées par le système informatique et pourront être accessibles, sous des strictes règles déontologiques, pour des raisons techniques ou en cas de soupçon de malveillance. Dans ce dernier cas, le service Ressources Humaines en sera informé préalablement.

La protection du matériel et des informations contre le vol, la copie et la dégradation doit être assurée en permanence. Le matériel mobile et les données liées sont de la responsabilité de l'utilisateur.

Tous les ordinateurs doivent être attachés par un câble de sécurité ou rangés sous clé. Le câble de sécurité est livré par le RSI au moment de la livraison du matériel portable. Le détenteur d'un matériel doit en permanence être en mesure de justifier de la propriété du matériel et des informations.

En cas de vol d'un matériel ou d'information, le détenteur doit déposer une plainte auprès des autorités, informer immédiatement le RSI et son responsable hiérarchique.

En cas de travail dans un lieu public (tel qu'une gare, un train, un avion ou dans la rue), l'utilisateur doit veiller à ne pas dévoiler d'informations confidentielles ou secrètes en utilisant des moyens de protection d'écran mis à sa disposition.

5. Règles d'utilisation des moyens informatique

Les moyens informatiques sont attribués à des fins professionnelles.

Néanmoins, l'usage à des fins privées des moyens informatiques mis à la disposition du salarié, est toléré à condition que cet usage :

- Soit occasionnel et raisonnable
- N'entrave en rien la bonne conduite des missions
- N'entrave pas la productivité
- N'ait pas d'impact négatif sur l'image de l'entreprise
- Ne constitue pas une infraction aux présentes instructions ; Ne constitue pas une infraction aux lois françaises.

Les dispositions légales, le règlement intérieur, les contrats de travail s'appliquent pleinement même lors d'un usage personnel.

L'utilisateur qui souhaite utiliser, à des fins privées, les moyens informatiques mis à sa disposition est tenu de l'indiquer clairement grâce aux termes « Personnel » ou « Privé » dans le titre, l'objet ou l'intitulé. Cette mention doit obligatoirement apparaître dans le nom des fichiers ou répertoires ou dans le sujet des messages concernés.

Toutes les informations qui ne sont pas clairement identifiées comme « Personnel » ou « Privé », sont considérées comme des informations professionnelles.

5.1 Accès à 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 prohibé par le Service Informatique. Celui-ci est habilité à imposer des configurations du navigateur et à restreindre le téléchargement de certains fichiers

La consultation des réseaux sociaux et la contribution des utilisateurs à des forums de discussion, systèmes de discussion instantanée, blogs, sites pendant le temps de travail, doit rester exceptionnelle. L'utilisateur ne pourra s'inscrire à ces réseaux sociaux avec son adresse mail ASSURMER, à l'exception de ceux qu'ils utilisent à titre professionnel comme Linkedln, Twitter (le cas échéant). L'utilisateur sera attentif à ne pas prendre de postions engageant l'entreprise ou sa réputation.

Il est rappelé que les utilisateurs ne doivent en aucun cas se livrer à une activité illicite ou portant atteinte aux intérêts de l'entreprise, y compris sur Internet.

5.2 Messagerie électronique

Chaque salarié dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique attribuée par le Service Informatique.

Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Les utilisateurs sont invités à informer le RSI des dysfonctionnements qu'ils constatent dans le dispositif de filtrage.

L'attention des utilisateurs est attirée sur le fait qu'un message électronique a la même portée qu'un courrier manuscrit et peut rapidement être communiqué à des tiers.

L'envoi de messages électroniques à des tiers obéit aux mêmes règles que l'envoi de correspondances postales, en particulier en termes d'organisation hiérarchique.

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

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, le cas échéant, l'opportunité de mettre en copie cachée les destinataires d'un même mail, 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, l'existence d'archives accessibles par le public et les modalités d'abonnement. Les règles de conduite définies par la Directive Européenne RGPD entrée en application le 25 mai 2018 doivent impérativement être respectées.

La vigilance des utilisateurs doit redoubler en présence d'informations à caractère confidentiel. Les messages doivent dans ce cas être cryptés.

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, injurieux, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire.

L'utilisateur ne doit également pas :

- Relayer des messages de fausse alerte
- Participer à des chaînes de messages
- Intercepter, modifier et transférer à d'autres personnes ni rendre publiques les communications qui ne lui sont pas adressées.

La forme des messages professionnels doit respecter les règles définies par la politique de communication, notamment en ce qui concerne la mise en forme et la signature des messages.

L'envoi de messages en masse ou à l'ensemble des collaborateurs doit être effectué avec grande modération.

Le RSI doit être informé de toute absence imprévue supérieure à deux jours afin de pouvoir mettre en place, le cas échéant, un message d'absence et rediriger ainsi les interlocuteurs.

Les messages à caractère personnel sont autorisés, à condition de respecter la législation en vigueur, de ne pas perturber et de respecter les principes posés dans la présente charte :

- Être signalés par la mention « personnelle » ou « privée » dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé " Personnel"
- Classés, dès réception, dans un dossier lui-même dénommé " Personnel ". En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.

Pour autant, les utilisateurs sont invités, dans la mesure du possible, à utiliser leur messagerie personnelle pour l'envoi de message à caractère personnel.

Enfin, afin d'éviter l'interception de tout message destiné aux élus, ceux-ci doivent être signalés et classés de la même manière que les messages à caractère personnel.

5.3 Assistance

En cas d'incident ou d'anomalies, les utilisateurs doivent se rapprocher de l'équipe informatique selon la gestion des incidents pratiquée. Seul le Service Informatique est habilité à réaliser et à suivre les opérations de dépannage.

L'utilisateur concerné est chargé d'assurer l'accès des intervenants à son matériel, d'organiser le rendez-vous avec l'intervenant du Service Informatique et de l'informer des résultats de l'intervention.

6. Limites techniques

Des espaces de stockage sont mis à la disposition des utilisateurs sur les serveurs de l'entreprise. Ces espaces comportent des zones nominatives et des zones partagées. Ces espaces sont réservés au stockage de documents professionnels. La taille d'espace disponible pour chaque zone de stockage est limitée.

L'utilisation doit :

- Respecter les limites de taille définies et régulièrement archiver les documents inutiles ou obsolètes
- Ne pas utiliser les espaces communs à des fins personnelles ou privées.

Pour des raisons techniques, l'envoi de messages électroniques n'est possible, directement, que vers un nombre limité de destinataires. Cette limite est susceptible d'être levée temporairement ou définitivement sur demande adressée au RSI. Des listes de diffusion sont ouvertes sur demande des utilisateurs par le Service Informatique.

De même, la taille, le nombre et le type des pièces jointes peuvent être limités par le Service Informatique pour éviter l'engorgement du système de messagerie.

Les messages électroniques sont conservés pendant une durée de 10 ans. Passé ce délai, ils sont automatiquement archivés ou supprimés. Si le salarié souhaite conserver des messages au-delà de ce délai, il lui appartient d'en faire une demande au RSI.

7. Contrôle des activités

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 de multiples traitements sont réalisés afin de surveiller l'activité du système d'information et de communication. Sont notamment surveillées et conservées les données relatives :

- A l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications suppression de fichiers ;

Aux connexions entrantes et sortantes au réseau interne, à la messagerie et à Internet, pour détecter les anomalies liées à l'utilisation de la messagerie et surveiller les tentatives d'intrusion et les activités, telles que la consultation de sites web ou le téléchargement de fichiers.

L'attention des utilisateurs est attirée sur le fait qu'il est ainsi possible de contrôler leur activité et leurs échanges. Des contrôles automatiques sont susceptibles d'être effectués pour limiter les dysfonctionnements, dans le respect des règles en vigueur. A ce stade, le contenu de l'information transférée (ex : par email) ou utilisé (ex : via internet) ne sera pas consulté par le service informatique.

En cas de dysfonctionnement constaté par l'équipe informatique, il peut être procédé, en lien étroit avec le service des Ressources Humaines et des organes de gouvernance de ASSURMER, à un contrôle manuel et à une vérification de toute opération effectuée par un ou plusieurs utilisateurs, incluant le cas échéant le contrôle du contenu des informations concernées.

Lorsque le contrôle porte sur les fichiers d'un utilisateur et sauf risque ou événement particulier, l'équipe informatique n'ouvrira pas des fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment contacté par le Service des Ressources Humaines (appel téléphonique + email).

Le contenu des messages à caractère personnel des utilisateurs (tels que définis à l'article 4 des présentes), ne peut en aucun cas être contrôlé par l'équipe informatique.

8. Exploitation des moyens informatiques

Ce paragraphe concerne les droits et devoirs des personnels informatiques disposant d'accès privilégiés au système d'information (ci-après administrateurs techniques).

9. Obligation de discrétion

Afin de garantir le bon fonctionnement et la sécurité des moyens informatiques, un nombre réduit de personnes, chargées de leur administration dispose d'un accès privilégié sur ceux-ci. Ces personnes encore nommées administrateurs techniques ont notamment la possibilité d'accéder aux fichiers et courriers électroniques stockés et échangés.

Conformément aux lois en vigueur dont la loi 78-17 relative à l'informatique, aux fichiers et aux libertés, ces personnes sont soumises à une obligation de secret professionnel. Elles ne peuvent en aucun cas exploiter à des fins autres que celles liées au bon fonctionnement et à la sécurité des moyens informatiques, les informations dont elles auraient eu connaissance.

En cas de force majeure, les Gérants d'ASSURMER et le RSI peuvent demander à la production informatique l'accès aux informations ou aux boites aux lettres d'utilisateurs. Le service des Ressources Humaines en est informé. Dès lors, l'administrateur technique prend la responsabilité de respecter les lois en vigueur (notamment le code du travail et la loi informatique et libertés) et le §7.4.3. L'administrateur technique doit respecter le caractère personnel des informations dès l'instant que cela est explicitement indiqué.

9.1 Droits et devoirs spécifiques aux administrateurs spécifiques

Les administrateurs :

- Ont la charge de la bonne qualité des services du Service Informatique fournis aux utilisateurs dans la limite des moyens alloués. Ils ont le droit d'entreprendre toute démarche nécessaire au bon fonctionnement des moyens informatiques en accord avec le RSI
- Ont le devoir d'informer, dans la mesure du possible, les utilisateurs de toute intervention nécessaire, susceptible de perturber ou d'interrompre l'utilisation habituelle des moyens informatiques
- Ont le devoir d'informer immédiatement le RSI de toute tentative d'intrusion sur un système, ou de tout comportement délictueux d'un utilisateur
- Ont l'obligation de préserver et de respecter la confidentialité des informations privées qu'ils sont amenés à connaître dans le cadre de leur activité
- Doivent avoir la connaissance et la maîtrise de tous les équipements informatiques et réseaux appartenant au sous-réseau qu'ils gèrent. Ils doivent tenir à jour la liste des équipements (machines, routeurs, imprimantes, . . .) et des prises réseaux (localisation, utilisateur connecté à la prise)
- Doivent inspecter régulièrement les fichiers de traces de manière à détecter le plus vite possible toute intrusion. Toute création de nouveau service, ouverture de nouveaux ports doit être validée par le RSI
- Ont le devoir d'appliquer les correctifs nécessaires aux applications qui présentent des failles de sécurité
- Ont le devoir de s'informer régulièrement sur les menaces qui pèsent sur le SI de l'entreprise et des mesures de sécurité mises en place par l'entreprise
- Doivent respecter toutes dispositions définies par le RSI.

9.2 Prise en main à distance

Les logiciels de prise de main à distance permettent notamment aux administrateurs d'accéder à distance à l'ensemble des données de n'importe quel poste de travail, à des fins de maintenance informatique
Ces outils de télémaintenance ou de prise de main à distance ne doivent en aucun cas être utilisés à des fins de contrôle de l'activité des utilisateurs. Une telle utilisation n'étant ni conforme au principe de proportionnalité, ni respectueuse du principe de finalité posé par la loi « informatique et libertés »

Dans l'hypothèse d'un recours à ces outils à des fins de maintenance informatique par un administrateur, leur utilisation doit s'entourer de précautions afin de garantir la transparence dans leur emploi et la confidentialité des données auxquelles le gestionnaire technique accédera par ce moyen, dans la stricte limite de ses besoins

Doivent notamment figurer au titre de ces précautions :

- L'information préalable et le recueil de l'accord de l'utilisateur pour « donner la main » à l'administrateur informatique avant l'intervention sur son poste (à titre d'illustration, l'accord peut être donné par simple validation d'un message d'information apparaissant sur son écran)
- La traçabilité des opérations de maintenance (par exemple, par la tenue d'un registre des interventions), ainsi que la précision dans les contrats des personnes assurant la maintenance - notamment en cas de recours à des prestataires extérieurs - de leur obligation de n'accéder qu'aux données informatiques nécessaires à l'accomplissement de leurs missions et d'en assurer la confidentialité.

10. Données personnelles

Si l'utilisateur est amené à constituer des fichiers soumis aux dispositions de la loi informatique et libertés, dans le cadre de son activité professionnelle, il doit accomplir les formalités requises par le RGPD en concertation avec son management et le RSI, et veiller à un traitement des données conforme aux dispositions légales.

L'utilisateur dispose d'un droit d'accès, de modification et de suppression des informations à caractère personnel le concernant conformément aux dispositions légales.

11. Gestion des absences ou des départs définitifs

En cas d'absence ou de départ définitif de l'entreprise, l'utilisateur est tenu de communiquer à sa hiérarchie les données et informations nécessaires à la poursuite de l'activité de la société (messagerie et fichiers notamment).

En cas d'impossibilité ou de refus de la part de l'utilisateur, l'entreprise peut prendre les mesures nécessaires pour accéder aux données professionnelles contenues sur les ressources informatiques et/ou services internet de l'intéressé.

Il appartient à l'utilisateur lors de son départ définitif de l'entreprise de sauvegarder ses données privées et uniquement celles-ci, sur une clef USB, puis de les détruire sur le réseau informatique de

l'entreprise. Au cas où les circonstances du départ ne permettraient pas d'atteindre cet objectif, l'entreprise conservera une sauvegarde de ses fichiers pour une durée de 30 jours calendaires sans engagement de résultat.

12. 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 salarié, celui-ci est informé dans un bref délai des faits qui lui sont reprochés, sauf risque ou événement particulier et dans le respect de la procédure disciplinaire et des droits de la défense.

Chaque utilisateur doit se conformer à la politique de sécurité des systèmes d'information de l'entreprise.

L'entreprise se réserve le droit de prendre toute mesure pratique dans le respect du cadre légal afin d'établir les responsabilités en cause et d'empêcher toute utilisation irrégulière ou illégale des systèmes.

Il est rappelé que les droits d'accès aux moyens informatiques ainsi que les conditions d'utilisation sont accordés à chaque utilisateur en considération stricte des fonctions qu'il occupe. L'utilisateur est informé que toute tentative de s'arroger des accès indus à des systèmes informatiques, toute manipulation technique déloyale ou divulgation d'informations préjudiciables à un tiers ou à l'entreprise, tout usage volontairement contraire aux règles internes ou aux lois constituent une faute pouvant entraîner des sanctions et engager sa responsabilité individuelle.

13. Entrée en vigueur

Les dispositions de la présente Charte sont intégrées et annexées au règlement intérieur d'ASSURMER.

La présente Charte a été :

- Soumise à l'avis du CSE
- Communiquée à L'Inspecteur du Travail
- Déposée au secrétariat du greffe du Conseil des Prud'hommes de Montpellier.

Elle est affichée sur les panneaux de la direction et publiée sur le portail RH, et remise à tout nouvel entrant contre décharge.

La présente Charte entre en vigueur dans les délais prévus par la loi après l'accomplissement des formalités de publicité et de dépôt, soit le 03 octobre 2022.

Fait à Montpellier le 01 septembre 2022.

La Gérance