All you need. **With love.**

ANNEXE 3 - AU REGLEMENT INTERIEUR

Charte d'utilisation des Moyens Informatiques et des Outils Numériques

Sommaire

1. Introduction

Manutan met à la disposition de ses salariés et de certains intervenants externes des équipements informatiques (micro-ordinateur, imprimante, logiciels...), des moyens de communication (messagerie, accès Internet, téléphone fixe et/ou mobile...) ainsi que des informations et données (bases de données, images, vidéos...) nécessaires à l'accomplissement de leur mission.

Chaque utilisateur doit être conscient que, d'une part, l'usage de ces ressources obéit à des règles qui s'inscrivent dans le respect de la loi et d'un usage approprié, représentant ainsi un gage d'efficacité opérationnelle, et que, d'autre part, sa négligence ou sa mauvaise utilisation des ressources fait encourir des risques à l'ensemble de l'entreprise.

La charte, annexée au règlement intérieur de l'entreprise, a pour objet de préciser la responsabilité des utilisateurs afin d'instaurer un usage correct du système d'information et de communication.

2. Champ d'application de la charte

La présente charte s'applique à l'ensemble des collaborateurs de Manutan et aux personnes, permanentes ou temporaires, utilisant les moyens informatiques de l'entreprise que ce soit à partir du réseau administré par l'entreprise ou par un accès à distance.

Les salariés veillent à faire accepter valablement les règles posées dans la présente charte à toute personne à laquelle ils permettraient d'accéder au système d'information et de communication.

Dans tous les cas, les interdictions prévues dans la présente charte d'utilisation des Moyens Informatiques et des Outils Numériques s'appliquent sous réserve des droits reconnus par la loi, aux représentants du personnel et aux délégués syndicaux.

La présente charte est sans préjudice des accords particuliers pouvant porter sur l'utilisation du système d'information et de communication par les institutions représentatives, l'organisation d'élections par voie électronique ou la mise en télétravail.

3. Définitions

On désignera de façon générale sous le terme « Ressources Informatiques », l'ensemble des matériels informatiques (ordinateurs fixes ou portables, serveurs, imprimantes, photocopieurs...), les logiciels et les matériels de communication (téléphones fixes et/ou mobiles, télécopieurs...) ainsi que les fichiers, données et bases de données accessibles localement ou à distance

On désignera par « Services Internet », la mise à disposition par des réseaux locaux ou distants de moyens d'échanges et d'informations diverses : Web, messagerie, forum, intranet ...

On désignera sous le terme « utilisateur », les personnes ayant accès ou utilisant les ressources informatiques et services Internet.
On désignera sous le terme « entreprise » les différentes entités du groupe MANUTAN présentes sur le site de Gonesse.

4. Principes généraux

La Direction des Systèmes d'Information 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 l'utilisation des ressources mises à disposition des utilisateurs.

La Direction des Systèmes d'Information 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. Les membres du service informatique 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.

4.1 Utilisation des outils numériques dans le cadre professionnel

L'utilisation des ressources informatiques et l'accès à internet doivent être effectués exclusivement à des fins professionnelles. Leur utilisation à des fins personnelles peut toutefois être tolérée, dans le cadre d'une utilisation « raisonnable ». C'est-à-dire :

- Que l'utilisation du système à titre extraprofessionnel ne se fasse pas au détriment des tâches professionnelles incombant au collaborateur.
- Que l'utilisation du courrier électronique n'affecte pas le trafic normal des messages professionnels.
- Que l'utilisation d'internet n'entrave pas l'accès professionnel.

Pour des raisons de sécurité, l'accès à certains sites peut être limité ou prohibé par la Direction des Systèmes d'Information. Celui-ci est habilité 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 est interdite sauf autorisation préalable du service informatique. Un tel mode d'expression est susceptible d'engager la responsabilité de l'entreprise, une vigilance renforcée des utilisateurs est donc indispensable.

4.2 Protection des informations de l'entreprise

L'utilisateur a accès aux informations et documents conservés sur son ordinateur ou sur le réseau interne de l'entreprise dans les répertoires autorisés des dossiers publics ou partagés.

L'utilisateur doit assurer la protection des informations auxquelles il accède et il est responsable des droits qu'il donne aux autres utilisateurs internes ou externes. Il doit notamment :

- Protéger ses données en utilisant les différents moyens de sauvegarde individuels ou mis à sa disposition.
- Ne pas transmettre des documents de l'entreprise ni les déposer sur des serveurs externes sans y être autorisés par les responsables habilités.
- S'assurer de ne pas laisser à disposition, dans un bureau ouvert ou sur une imprimante, des documents ou supports informatiques contenant des données confidentielles.

Par ailleurs, il est interdit de tenter par un procédé frauduleux de lire, modifier, copier ou détruire les données autres que celles qui lui appartiennent en propre, directement ou indirectement.

4.3 Respect de la loi Informatique et Libertés et de la Règlementation Européenne sur la Protection des Données Personnelles

Tout besoin d'utilisation d'un fichier tombant sous le coup de la loi « Informatique et Libertés » ou du Règlement Général sur la Protection des Données (RGPD/GDPR) devra donner lieu auparavant à une déclaration à la CNIL en concertation, le cas échéant, avec son manager ou le Directeur des Systèmes d'Information et en avoir reçu l'autorisation.

4.4 Respect des règles de bon usage et de sécurité

Tout utilisateur doit utiliser les ressources informatiques de façon rationnelle et loyale afin d'en éviter la saturation ou le détournement à des fins personnelles. À son niveau, il doit contribuer à la sécurité générale du système d'information et aussi à celle de l'entreprise.

En particulier, l'utilisateur doit :

- Faire preuve de la plus grande correction à l'égard des interlocuteurs dans les échanges électroniques par courrier, forum de discussions...
- Ne pas émettre d'opinions personnelles susceptibles de porter préjudice au groupe Manutan.
- Ne pas utiliser le système d'information à des fins personnelles lucratives ou non, à des fins de promotion, de publicité ou de démarchage.
- Appliquer les recommandations de sécurité du service auquel il appartient.

4.5 Respect du droit d'auteur

Il est interdit de communiquer intégralement ou partiellement une œuvre ou sa reproduction au public sans autorisation préalable du ou des auteurs. Les logiciels, les bases de données et autres créations telles que les articles, photographies, pages WEB, fichiers musicaux ou vidéos, etc. constituent notamment des œuvres au sens du code de la propriété intellectuelle.

Il est également interdit, même lorsque l'œuvre a été divulguée par son auteur, d'en effectuer des copies ou reproductions (en dehors du droit à la copie privée ou de sauvegarde qui implique l'obligation de détention d'un exemplaire de l'œuvre acquis légalement, ou dans le cadre de l'utilisation de logiciels libres). Cette interdiction peut être levée par l'autorisation de l'auteur ou/et de l'éditeur/producteur.

L'usage d'un logiciel suppose, en général, la détention d'une licence. Les éventuelles copies de logiciels doivent être strictement conformes aux engagements pris par l'entreprise dans le contrat de licence.

4.6 Respect du droit à l'image et du droit à la vie privée

En application de l'article 226-1 du code pénal, l'utilisateur s'engage à :

- Ne pas diffuser d'informations portant atteinte à la vie privée de tierces personnes.

- Ne pas diffuser d'images sans l'autorisation des personnes concernées.
- Ne pas enregistrer ou diffuser d'enregistrements (voix, vidéo, etc.) de tierces personnes sans accord préalable des personnes concernées.

4.7 Respect du droit à la déconnexion du salarié

Conformément à l'article L. 2242-8 du Code du travail, le droit à la déconnexion peut se définir comme le droit de chaque salarié de ne pas être connecté à un outil numérique professionnel pendant ses temps de repos et de congés. Il convient également de préciser que chaque salarié a un devoir de déconnexion, qui se définit par la responsabilité individuelle du bon usage des outils numériques, qui ne doit pas être seulement le résultat d'une injonction de la hiérarchie.

Il convient de souligner la nécessité de veiller à ce que l'usage des outils numériques :

- Respecte la qualité du lien social au sein des équipes et ne devienne pas un facteur conduisant à l'isolement des salariés sur leur lieu de travail.
- Garantisse le maintien d'une relation de qualité et de respect du salarié tant sur le fond que sur la forme de la communication.
- Ne devienne pas un mode exclusif d'animation managériale, et de transmission des consignes de travail.
- Respecte le temps de vie privée du salarié.

Chaque salarié, quel que soit son niveau hiérarchique, veillera à se déconnecter du réseau et dans la mesure du possible à limiter l'envoi de courriel en dehors des heures habituelles de travail et dans le cas contraire, d'utiliser les possibilités d'envois différés proposés par les outils numériques de l'entreprise.

En cas de circonstances particulières, nées de l'urgence et de l'importance des sujets traités, des exceptions à ce principe seront évidemment mises en œuvre.

Les salariés en déplacement à l'étranger appliqueront ces mesures selon l'horaire de travail local propre à la mission. Ils essayeront dans la mesure du possible de tenir compte du décalage horaire pour l'envoi de leurs messages afin que les destinataires reçoivent les messages dans le créneau horaire de leur travail.

Les salariés ayant reçu un message en dehors de leurs horaires habituels de travail ne sont pas tenus d'en prendre connaissance avant le prochain horaire de travail.

5. Dispositions particulières

5.1 Mise à disposition du matériel informatique

L'entreprise met à disposition de l'utilisateur les ressources informatiques nécessaires à l'accomplissement de ses missions.

L'utilisateur est responsable du matériel mis à sa disposition. Il doit notamment :

- Utiliser le matériel en respectant les consignes d'utilisation.
- Manipuler le matériel avec tout le soin nécessaire.
- Sécuriser le matériel chaque fois que cela est nécessaire (câble de sécurité, locaux fermés...).

Prise de main à distance d'un poste utilisateur

Pour des nécessités de maintenance, la Direction des Systèmes d'Information, ou un prestataire mandaté, a la possibilité de prendre la main à distance du poste de travail d'un utilisateur.

Renouvellement du matériel

Le renouvellement du matériel est fait à l'initiative de la direction selon les règles de l'entreprise. Sauf disposition particulière, le renouvellement d'un matériel entraîne la restitution de l'ancien matériel.

Une demande de remplacement avant le terme prévu doit être validée par le ou les directeurs concernés.

Restitution du matériel

Lors du départ de l'utilisateur, le matériel doit être restitué au service « Business Desk » de la Direction des Systèmes d'Information.

Vol du matériel

La disparition du matériel doit être immédiatement signalée au service « Business Desk » de la Direction des Systèmes d'Information.

5.2 Identification dans le système d'information

Pour accéder au système d'information de l'entreprise, l'utilisateur doit s'authentifier grâce à un identifiant personnel et un mot de passe. Toutes les opérations réalisées sous cet identifiant engagent son propriétaire.

L'utilisateur doit choisir un mot de passe sûr qui doit être gardé confidentiel. En tout état de cause, les paramètres de connexion (identifiants et mots de passe) ne doivent pas être communiqués à des tiers internes ou externes. Ils ne doivent pas être aisément accessibles et doivent être saisis à chaque accès et ne pas être conservés en mémoire dans le système d'information.

L'utilisateur doit :

- Ne pas quitter son poste de travail sans verrouiller ou déconnecter sa session, ou en laissant des ressources / services accessibles.
- Signaler toute tentative de violation de son compte et, de façon générale, toute anomalie qu'il peut constater.
- S'engager 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 pas utiliser ou essayer d'utiliser des comptes autres que le sien.
- Ne pas tenter de masquer son identité.
- Ne pas usurper l'identité d'une autre personne et il ne doit pas intercepter de communications entre tiers.

5.3 Connexion d'un matériel au réseau de l'entreprise

Seuls les matériels fournis ou validés par la Direction des Systèmes d'Information sont autorisés à être connectés sur le réseau de l'entreprise.

Il est interdit de brancher sur le réseau tout matériel informatique n'appartenant pas à Manutan sans l'autorisation préalable de la Direction des Systèmes d'Information.

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 par la Direction des Systèmes d'Information. Toute autorisation prend fin lors de la cessation même provisoire de l'activité professionnelle ayant justifié cette autorisation.

Les exceptions :

- Accès internet : la connexion des matériels personnels est autorisée exclusivement selon la procédure d'accès prévue à cet effet (WIFI invité).
- L'accès à la messagerie et à l'agenda professionnel sur des terminaux personnels, à la condition où ceux-ci sont équipés d'un système d'exploitation et d'un logiciel anti-virus à jour (correctifs de sécurité, version logicielle et signatures) ainsi que d'un code d'accès de déverrouillage.

5.4 Installation / désinstallation d'un logiciel sur le poste de travail

Pour assurer la comptabilité des matériels et logiciels ainsi que le respect des droits d'usage, les logiciels sont installés sur les postes utilisateurs sous la responsabilité de la Direction des Systèmes d'Information.

En particulier, il est interdit :

- D'installer ou de désinstaller un logiciel sans l'accord de la Direction des Systèmes d'Information.
- 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.
- De désactiver les anti-virus.

5.5 Utilisation des services Internet

L'utilisateur doit faire usage des services Internet **dans le cadre exclusif de ses activités professionnelles** sauf exception visée au paragraphe 0 de la présente charte.

En particulier, il est interdit :

- D'utiliser les sites de streaming radio ou vidéo, (écouter une station de radio, regarder la télévision, visionner ou télécharger un film ou une vidéo...).
- De consulter des sites et des pages internet qui présentent un contenu relevant du droit pénal (tels que: pornographie, pédophilie, racisme, incitation à la violence ou à des crimes ou délits, discriminations...).
- De diffuser des documents en grand nombre (Spam).
- De copier des œuvres protégées par des droits d'auteur, de participer à des jeux de hasard, d'argent, ou de s'impliquer dans le blanchiment d'argent au moyen d'Internet.

En cas d'abus, la Direction des Systèmes d'Information pourra interdire l'accès aux sites n'ayant pas de caractère professionnel.

5.6 Utilisation de la messagerie professionnelle

L'entreprise met à disposition des salariés une boîte aux lettres électroniques professionnelle et nominative.

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. Ils doivent prendre garde à ne pas engager la responsabilité civile ou pénale de l'entreprise et/ou de l'utilisateur. Ils doivent également veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Ainsi, 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.

Le paramétrage de la boite aux lettres électroniques (transfert automatique, gestionnaires d'absence, droit d'accès en consultation ou en mise à jour) disponible dans les logiciels reste sous la responsabilité de l'utilisateur.

Il est recommandé :

- De maintenir son agenda électronique à jour.
- De renseigner le gestionnaire d'absence du bureau afin d'assurer de la continuité de service avant un départ planifié (congés, déplacement...).
- D'archiver régulièrement les messages afin de ne pas atteindre la taille limite de la boîte.
- De limiter la taille des messages et des pièces jointes, notamment en privilégiant les liens plutôt que les fichiers.
- De vérifier et de mettre à jour régulièrement les règles de routage des messages.

Accès à une boîte aux lettres électroniques

Pour les besoins de continuité de service, l'entreprise peut avoir accès aux messages contenus dans la boîte aux lettres électroniques en cas d'absence temporaire ou définitive de l'utilisateur.

L'accès à la messagerie se fait par initialisation du compte utilisateur et fourniture d'un nouveau mot de passe à la demande d'un supérieur hiérarchique auprès du Directeur des Systèmes d'Information et du Directeur des Ressources Humaines.

Au retour de l'utilisateur, le responsable hiérarchique l'informe des opérations réalisées sur le compte et la boîte aux lettres électroniques. L'utilisateur doit s'assurer que le paramétrage du logiciel est bien conforme à ses intentions et le modifier si nécessaire.

Accès aux messages personnels

Il n'est pas autorisé pour une personne autre que le titulaire du compte de consulter les messages ou les répertoires portant explicitement la mention « 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 signalés par la mention « Personnel » dans leur objet et être classés dès l'envoi ou la réception dans un dossier lui-même dénommé « Personnel ». En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.

5.7 Utilisation de la téléphonie

Les téléphones (fixes ou portables) sont des outils mis à la disposition de l'utilisateur à titre professionnel. Il doit donc en faire un usage approprié. Un usage occasionnel, à titre personnel, est toléré dans les limites du raisonnable.

Un contrôle est effectué sur les appels sortants et, en cas de doute sur leur utilité professionnelle, une justification pourra être demandée au salarié. En cas d'utilisation personnelle avérée, le montant des communications sera facturé au salarié.

Il est à noter que certaines informations sur les communications sont mémorisées (numéro appelé, durée, numéro de poste appelant).

Un système d'écoute et/ou d'enregistrement des communications des salariés en contact avec les clients est susceptible d'être utilisé dans un but de formation et de contrôle de la qualité du service téléphonique rendu. Dans tous les cas, les utilisateurs concernés seront préalablement informés de sa mise en œuvre et pourront prendre connaissance du compte-rendu de la conversation écoutée/enregistrée et formuler leurs observations. Les enregistrements effectués ne seront conservés que durant le délai strictement nécessaire à l'objectif poursuivi.

5.8 Utilisation d'applications externes (SaaS & Cloud)

Seuls les services fournis ou validés par la Direction des Systèmes d'Information sont autorisés à être manipulés par les utilisateurs.

La souscription à un service non disponible via les outils internes de l'entreprise sera soumise à la validation de la Direction des Systèmes d'Information. Celle-ci devant notamment s'assurer de la conformité dudit service avec la Réglementation Européenne sur la Protection des Données Personnelles.

Dans le cas où le service est validé par la Direction des Systèmes d'Information, l'usage d'un compte personnel sur ledit service à des fins professionnelles n'est pas autorisé. Le compte d'accès devra être géré (création/suppression) par le service « Business Desk » de la Direction des Systèmes d'Information.

5.9 Utilisation du système d'information par les Institutions Représentatives du Personnel

Le matériel mis à disposition par l'entreprise est sous la responsabilité de chaque Institution Représentative du Personnel qui devra remplacer à l'identique le matériel ayant fait l'objet d'une détérioration.

Il ne peut être utilisé d'autres matériels que ceux compatibles avec le système informatique de l'Entreprise.

Toute installation d'un logiciel doit se faire avec l'accord préalable du service informatique.

L'envoi de tous tracts et messages en nombre aux salariés par les Institutions Représentatives du Personnel est interdit.

Afin d'éviter l'interception de tout message destiné à une institution représentative du personnel, les messages présentant une telle nature doivent être signalés et classés de la même manière que les messages à caractère personnel.

Pour garantir la confidentialité des échanges électroniques éventuels des salariés avec les organisations syndicales, chaque représentant du personnel élu par les salariés ou désigné par les Organisations Syndicales peut disposer d'une messagerie spécifique qui sera utilisée dans le cadre de son ou ses mandat(s). S'il ne souhaite pas utiliser cette messagerie, il devra le faire savoir par écrit à la Direction des Ressources humaines et

prendre alors les dispositions nécessaires pour assurer la confidentialité des échanges électroniques qui ont un lien avec son (ses) mandat(s).

5.10 Préservation de l'intégrité des systèmes informatiques

L'utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des systèmes informatiques et des réseaux que ce soit par des manipulations anormales du matériel (ex. éteindre son PC autrement que par l'arrêt logiciel) ou par l'introduction de logiciels parasites (ex. virus, chevaux de Troie...).

Accès aux ressources de tiers

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.

De même, il ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède.

6. Audits et contrôles

En cas de dysfonctionnement constaté par la Direction des Systèmes d'Information, 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, la Direction des Systèmes d'Information ne peut ouvrir les fichiers ou les messages identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur ou dans sa messagerie professionnelle qu'en présence de ce dernier ou celui-ci dûment appelé.

6.1 Les matériels

Pour les besoins de maintenance et de gestion du parc, les matériels mis à disposition des utilisateurs intègrent des logiciels traçant les modifications de configurations ainsi que l'installation de logiciels.

La Direction des Systèmes d'Information, ou les prestataires mandatés par elle, peuvent accéder à ces informations en cas de comportement anormal du système ou dans le cadre d'audits.

6.2 Les logiciels

Les logiciels utilisés par l'entreprise permettent la traçabilité des opérations réalisées par l'utilisateur.

La Direction des Systèmes d'Information, ou le prestataire mandaté par elle, peut accéder à ces informations en cas de comportement anormal du système pour en assurer la maintenance ou dans le cadre d'audits.

6.3 Internet

La Direction des Systèmes d'Information, ou le prestataire mandaté par elle, réalise un suivi du trafic internet à des fins de statistiques, de qualité de service et de sécurité. La supervision et les vérifications par des audits sont réalisées dans les limites prévues par la loi.

Dans le cadre de la mise en place d'outils de protection du système d'information, il sera procédé au déchiffrement TLS/SSL (Transport Layer Security) des flux entrants et sortants afin d'identifier des logiciels malveillants, de protéger le patrimoine informationnel ou encore de détecter des flux sortants anormaux.

Toutes les opérations réalisées sur Internet sont enregistrées et peuvent être vérifiées en cas de soupçon d'abus.

En cas d'enquête initiée en interne, l'utilisateur concerné est prévenu préalablement par son manager puis informé du résultat des investigations.

6.4 Messagerie

La Direction des Systèmes d'Information, ou le prestataire mandaté par elle, réalise un suivi du trafic des messages à des fins de statistiques, de qualité de service et de sécurité. La supervision et les vérifications par des audits sont réalisées dans les limites prévues par la loi.

Toutes les opérations réalisées sur la messagerie sont enregistrées pour une durée maximum de 12 mois et peuvent être vérifiées en cas de soupçon d'abus.

En cas d'enquête initiée en interne, l'utilisateur concerné est prévenu préalablement par son manager puis informé du résultat des investigations.

7. Sanctions

Le non-respect de ces règles est susceptible de justifier la suspension immédiate de l'utilisation du système d'information, et/ou le lancement de procédures disciplinaires. Certains de ces comportements seront susceptibles de poursuites pénales.

Dans le cas d'une mise en danger volontaire de la sécurité du système informatique, l'entreprise se donne le droit de poursuivre l'employé pour fautes graves afin d'obtenir le licenciement et des dommages et intérêts proportionnels à la faute commise. Il s'expose donc à des poursuites civiles et/ou pénales conformément aux textes en vigueur.

L'utilisation des logiciels (source ou binaire) et plus généralement de tout document (fichier, image, son, etc.) faite de manière non conforme au code de la propriété intellectuelle est susceptible de constituer un délit de contrefaçon, lequel est sanctionné par une amende de 300 000 € et de trois ans de prison.

8. Entrée en vigueur et formalités administratives

La présente Charte est annexée au Règlement intérieur de l'UES Manutan dont elle fait partie intégrante.

Conformément aux prescriptions de l'article L. 1321-4 du Code du travail, la Charte d'utilisation des Moyens Informatiques et des Outils Numériques a été :

- soumise pour avis au Comité d'Entreprise le 5 mars 2018 et, pour les matières relevant de sa compétence, au CHSCT le 5 mars 2018;
- communiquée en double exemplaire à l'inspecteur du travail dont dépend la société, accompagnés des avis formulés par les membres du CE et du CHSCT.
- déposée en un exemplaire au secrétariat du conseil des prud'hommes de Montmorency.

Elle est portée à la connaissance du personnel par voie d'affichage.

La Charte d'utilisation des Moyens Informatiques et des Outils Numériques a été rédigée dans l'intérêt de Manutan et de chacun des utilisateurs. Elle sera régulièrement mise à jour par la Direction des Systèmes d'Information de Manutan pour tenir compte de l'évolution constante de l'environnement et des techniques informatiques.