BK Consulting

CHARTE INFORMATIQUE

Date: 31/12/2019

Paraphe

RA

1. Objectif 2
2. Utilisateurs Concernes 2
3. Régles Générales d'utilisation 3
    3.1. Droits et Devoirs des Utilisateurs 3
    3.2. Droits et Devoirs de la Société 5
4. Poste de travail 5
    4.1. Mots de passe 6
    4.2. Dossiers -fichiers personnels 6
5. Messagerie électronique 6
    5.1. Usage professionnel 6
    5.2. CONSEILS GENERAUX 7
    5.3. En cas d'absence au delà de 3 jours (en respect avec la charte de deconnexion) 7
    5.4. 'Avertissement légal' de fin d'email 7
    5.5. Usage personnel 8
    5.6. Représentants du personnel ou syndicaux 8
6. Internet 8
7. Réseaux Sociaux 9
8. Téléphone 10
9. CONFIDENTIALITE 10
10. Analyse et contrôle de l'utilisation des ressources 10
11. Contrôles automatisés 11
    11.1. Contrôles 11
    11.2. Procédure de contrôle manuel 12
    11.3. Déchiffrement SSL des sites HTTPS 12
12. Sanctions 12
13. INFORMATION DES UTILISATEURS 12
14. REVISION DE LA CHARTE 13
15. Entrée en vigueur 13

Paraphe
RA

1. OBJECTIF

La société BK CONSULTING met en œuvre un système d'information et de communication nécessaire à son activité.

La présente charte informatique s'applique à l'ensemble des utilisateurs du système d'information et de communication de la société.

Elle a pour objectif :

- de sensibiliser les utilisateurs aux exigences de sécurité, afin d'assurer notamment la sécurité de l'ensemble des données auxquelles ils ont accès
- d'attirer leur attention sur certains comportements de nature à porter atteinte à l'intérêt de l'entreprise
- et de rappeler les sanctions prévues en cas de non-respect des règles applicables.

Ce document répertorie les règles relatives à l'utilisation du système d'information et de communication de l'entreprise (ressources): logiciels métiers, bureautique, messagerie, micro-ordinateurs fixes et portables, périphériques, téléphones fixes et portables, Internet, Extranet, Intranet, photocopieurs, abonnement à des services informatiques (liste non exhaustive).

2. UTILISATEURS CONCERNES

La présente charte s'applique à l'ensemble des personnes, permanents ou temporaires qui utilisent, à quelque titre que ce soit le système d'information et de communication de la société, y compris hors de l'entreprise à l'occasion du travail effectué pour le compte de celle-ci.

Elle s'applique ainsi à tous les salariés (y compris travaillant à l'étranger, à domicile, en déplacement, en mission chez des clients), aux stagiaires, intérimaires, salariés d'entreprises extérieures, prestataires extérieurs intervenant à quelque titre que ce soit, aux mandataires sociaux, visiteurs occasionnels.

Dès l'entrée en vigueur de la présente charte, chaque salarié s'en verra remettre un exemplaire, il devra en prendre connaissance et ~~à~~ devra la respecter et la faire respecter. Les ~~salariés~~ utillisateurs devront veiller à faire accepter valablement les présentes règles à toute personne à laquelle ils permettraient, sous autorisation, d'accéder aux systèmes d'information et de communication.

Cette charte ne remplace en aucun cas les lois en vigueur que chacun est censé connaître.

Paraphe

3. Regles Generales d'utilisation

3.1. Droits et Devoirs des Utilisateurs

L'utilisateur dispose de droits d'accès au système d'information. Ces droit d'accès sont strictement personnels et incessibles. Ils sont protégés par des paramètres de connexion que l'utilisateur doit garder strictement confidentiels. Aucun utilisateur ne doit se servir pour accéder au système d'information de l'entreprise d'un autre compte que celui qui lui a été attribué. Il ne doit pas non plus déléguer à un tiers les droits d'utilisation qui lui ont été attribués.

Les droits d'accès peuvent être modifiés, suspendus ou retirés à tout moment selon les besoins du service et prennent fin lors de la cessation de l'activité professionnelle pour le compte de l'entreprise.

L'utilisateur donne expressément son consentement pour que les données à caractère personnel le concernant et nécessaires à cet effet soient collectées dans le cadre des ouvertures de comptes d'accès aux applications et services de l'entreprise. Ces données ne seront utilisées que pour les finalités de ces inscriptions et leur utilisation.

Les ressources mises à disposition du salarié constituent un outil de travail. Chaque utilisateur est responsable des ressources qui lui sont confiées dans le cadre de ses fonctions, il doit en toute circonstance faire preuve de prudence et de vigilance et doit respecter les règles définies sur l'utilisation des ressources et notamment :

- Respecter en toute circonstances la legislation qui protège notamment les droits de propriété intelectuelle, le droit d'auteur, 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 à des contenus préjudiciables ;
- Ne pas stocker ou transmettre des informations, documents, photographies portant atteinte à la dignité humaine ou aux droits et images de chacun ou revêtant un caractère discriminatoire : faire référence à une quelconque appartenance à une ethnie, religion, race ou nation déterminée.
- Respecter l'intégrité et la confidentialité des données ;
- Ne pas perturber le bon fonctionnement du système informatique ;
- Ne pas introduire de matériel ou logiciel extérieurs, sauf accord de la Direction, et ne pas en utiliser ou connecter au système d'information et de communication de l'entreprise ;
- Ne pas sortir du matériel, logiciel, fichiers, données appartenant à l'entreprise sauf par obligations professionnelles et sous accord de la Direction.
- Ne pas installer de logiciels susceptibles de modifier la configuration des machines sans accord préalable de la Direction ;
- Utiliser les logiciels dans les conditions de licence soucrites par l'entreprise ;
- Respecter les contraintes liées à la maintenance du système d'information ;

Paraphe

- Ne pas masquer son identité ;
- Ne pas usurper l'identité d'autrui ;
- Ne pas appliquer de mesures de sécurité non validées par la Direction ;
- Informer immédiatement la Direction de toute perte, de toute tentative de violation ou anomalie relative à une utilisation de son compte d'accès, mais également de toute perte ou vol de son matériel informatique ou téléphonique, et de manière générale de tout risque d'atteinte à la confidentialité d'informations et/ou données de la société et/ou de ses clients et utilisateurs.
- Respecter la règlementation relative aux données à caractère personnel (notamment la Loi no 78-17 du 6 janvier 1978 modifiée ainsi que le Règlement européen 2016/679 du 27 avril 2016 général de relative à l'informatique) qui définit les conditions dans lesquelles des traitements de données personnelles peuvent être opérés ;
- Ne prendre aucune copie des données personnelles, à l'exception de celles nécessaires à l'exécution de son travail et dans le cadre de celui-ci, l'accord préalable de la Direction étant nécessaire ;
- Ne pas utiliser les données traitées à des fins autres que celles spécifiées dans son contrat;
- Ne pas divulguer ces données à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales;
- Prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques et données personnelles au cours de l'exécution de son contrat;
- Prendre toutes mesures de sécurité, notamment matérielles, pour assurer la conservation et l'intégrité des documents et informations traitées;
- Etre présent aux formations obligatoires concernant les sujets liés à la sécurité, la législation qui protège notamment les droits de propriété intellectuelle, le secret des correspondances, les données personnelles, la RGPD, la confidentialité des données et la lutte anti-corruption,
- Informer l'entreprise dès que possible en cas de faille de sécurité et à faire ses meilleurs efforts pour prendre toutes les mesures possibles pour neutraliser et en minimiser les impacts ;
- A la fin du contrat, restituer tout matériel et tous fichiers manuels ou informatisés stockant les données personnelles et informations saisies et n'en conserver aucune copie sur quelque support que ce soit;

Paraphe RA

3.2. Droits et Devoirs de la Societe

La Société s'engage à :

- Mettre à disposition des utilisateurs les ressources informatiques matérielles et logiciels nécessaires à la réalisation du travail ;
- Former l'utilisateur si nécessaire à la bonne utilisation des outils ;
- Informer les utilisateurs des perturbations éventuelles au bon fonctionnement du système informatique (maintenance...) ;
- Effectuer les mises à jour nécessaires des matériels et des logiciels utilisés;
- Définir les règles d'utilisation du système informatique et des moyens matériels mises à disposition des salariés et veiller à leur bonne application.

4. Poste de travail

Chaque utilisateur aura à sa disposition de nombreux outils informatiques, qu'il s'agisse de matériel (ordinateur portable, unité centrale, écran, clavier, souris), de système d'exploitation ou de logiciels (bureautique, communication, gestion, applications spécifiques) cette liste n'étant pas exhaustive. L'utilisateur est tenu de prendre soin du materiel informatique, et d'être vigilant lors de son utilisation.

L'utilisateur ne doit pas modifier les paramétrages de son poste de travail ou des différents outils mis à sa disposition, ni contourner les systemes de sécurité, notamment l'utilisateur doit s'assurer que, sur son ordinateur, les fonctionnalités de coupe-feu et de chiffrement des données du disque dur et du logiciel antivirus sont activées et à jour. En cas de besoin, il doit solliciter l'aide du responsable informatique.

Chaque utilisateur doit veiller à se prémunir contre le vol et la casse ; il ne doit pas user du matériel de manière frauduleuse ou négligente délibérément.

En cas d'absence même momentanée l'utilisateur doit verrouiller son ordinateur. Un verrouillage automatique au bout de 5 minutes maximum d'inactivité doit également être configuré. Cette précaution garantit la sécurité et la confidentialité de l'utilisation et des informations qu'il contient. L'utilisateur doit également vider les corbeilles et archiver les mails régulièrement et, ceci, au minimum chaque mois.

En fin de journée, l'utilisateur doit quitter l'ensemble des applications, arrêter le système informatique, éteindre écran et imprimante.

Paraphe
RA

4.1. Mots de passe

Des mots de passe sûrs, contenant au minimum 8 caractères et des caractères spéciaux, doivent être mis en place par l'utilisateur, conformément aux politiques proposées par les différents outils informatiques. Ces mots de passe doivent être changés tous les six mois, et ne pas être communiqués à une tierce personne. Ils ne doivent pas être écrits, ni utilisés dans plusieurs applications ou sites internet. Ils sont un outil nécessaire à la sécurité et la confidentialité des données.

4.2. Dossiers -fichiers personnels

Les dossiers, fichiers créés et archivés par l'utilisateur sur les outils professionnels (ordinateur fixe ou portable, téléphone portable, le réseau) mis à sa disposition par l'entreprise sont présumés avoir un caractère professionnel sauf si l'utilisateur les a expressément identifiés comme revêtant un caractère privé avec la mention "personnel" ou "privé" et classés comme tels dans un répertoire portant les mêmes mentions.
En l'absence d'une telle mention, les dossiers, fichiers sont supposés revêtir un caractère professionnel de telle sorte que l'entreprise est en droit de les ouvrir, même en l'absence du salarié.
Sauf circonstances exceptionnelles, risque ou évènement particulier, les fichiers, dossiers identifiés comme étant à caractère personnel et/ou privé ne pourront être ouverts qu'en présence du salarié ou celui-ci dument appelé et le cas échéant en présence d'un représentant du personnel.

5. Messagerie electronique

5.1. Usage professionnel

La messagerie électronique mise à disposition de l'utilisateur est réservée à des fins professionnelles. L'utilisation d'un pseudonyme ou d'un faux nom est expressément prohibée, sauf autorisation préalable de la Direction qui s'assurera du bien-fondé de cette utilisation.
L'utilisateur est tenu de consulter sa messagerie professionnelle d'une façon régulière durant les horaires de travail, exception faite des périodes d'absence.
Les messages électroniques sont en effet des outils de travail très importants. Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam.
L'utilisateur s'engage à s'occuper de la maintenance de sa messagerie électronique notamment en archivant les messages importants, en vidant périodiquement le dossier "éléments supprimés" et en archivant le contenu réguliérement.
Il est également recommandé à l'utilisateur de faire preuve de vigilance avant d'ouvrir une pièce jointe ou un lien présent dans un message électronique. En cas de doute (expéditeur

Paraphe RA

inconnu, message non attendu, URL suspecte...), l'utilisateur ne doit pas les ouvrir afin d'éviter tout acte de malveillance extérieur et supprimer l'email associé de sa messagerie (y compris du dossier "éléments supprimés").
Il est interdit d'utiliser un autre système de messagerie que celui mis à disposition, sauf accord de la Direction ;

5.2. CONSEILS GENERAUX

L'attention des utilisateurs est attirée sur le fait qu'un message électronique a la même portée et obéit aux mêmes règles que l'envoi des correspondances postales. Il convient de prendre garde au respect d'un certain nombre de principes, afin d'éviter les dysfonctionnements du système d'information, de limiter l'envoi de messages non sollicités et de ne pas engager la responsabilité civile ou pénale de la société BK CONSULTING et/ou de l'utilisateur.
Avant tout envoi, il est impératif de vérifier l'identité des destinataires du message et 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 l'opportunité de dissimuler certains destinataires, en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires.
La vigilance des utilisateurs doit redoubler en présence d'informations à caractère confidentiel.
Les utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle, des droits des tiers et de la règlementation sur les données à caractère personnel. 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.

5.3. EN CAS D'ABSENCE AU DELA DE 3 JOURS (EN RESPECT AVEC LA CHARTE DE DECONNEXION)

L'utilisateur s'engage à mettre en place un système de message automatique afin de mentionner son absence et la date de retour prévue afin de permettre notamment à un autre salarié de pouvoir gérer une urgence.

5.4. 'AVERTISSEMENT LEGAL' DE FIN D'EMAIL

L'utilisateur s'engage à intégrer après sa signature, dans tout email professionnel à usage externe, un "disclaimer" (avertissement relatif à la confidentialité des données et la responsabilité du récipiendaire) dont le modèle est installé par défaut sur la messagerie.

Paraphe RA

5.5. Usage personnel

Tout message électronique est réputé professionnel et est par conséquent susceptible d'être ouvert par un administrateur.
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.
Les messages personnels 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 personnels reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé « Privé ». Sauf circonstances exceptionnelles, risque ou évènement particulier, les messages signalés comme « privés » ne pourront être ouverts, qu'en présence du salarié ou celui-ci dument appelé et le cas échéant en présence d'un représentant du personnel.
En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.
La lecture de messages électroniques personnels reçus durant les heures de travail est tolérée si celle-ci reste occasionnelle et limitée. Elle ne doit en aucun cas entraver l'activité professionnelle.

5.6. Representants du personnel ou syndicaux

Afin d'éviter l'interception de tout message destiné aux représentants du personnel ou syndicaux, ces messages doivent comporter dans leur objet "IRP" ou "représentant du personnel" ou encore "CSE" et doivent être classés dans un dossier de cette même appellation.

6. Internet

L'utilisation d'internet est réservée aux utilisateurs à des fins professionnelles dans le cadre de l'exercice de leur fonction. Pour des raisons de sécurité ou de déontologie, l'accès à certains sites peut être limité ou prohibé par la Direction informatique qui est habilitée à imposer des configurations du navigateur et à installer des mécanismes de filtrage limitant l'accès à certains sites.
Il est toléré un usage modéré de l'accès à Internet pour des besoins personnels à condition que cet usage soit raisonnable en terme de durée et/ou de quantités de connections et que la navigation n'entraîne aucune conséquence préjudiciable pour l'entreprise.
En tout état de cause il est interdit de se connecter à des sites internet dont le contenu est contraire à l'ordre public, discriminatoire, portant atteinte aux bonnes moeurs, à la dignité humaine, ou à l'image de marque de l'entreprise, ainsi qu'à ceux pouvant comporter un risque pour la sécurité du système d'information de l'entreprise.

Paraphe RA

La contribution des utilisateurs à des forums de discussions instantanée, des blogs, des sites, dont l'usage est non profesionnel, est interdite sauf autorisation préalable de la Direction.
Les utilisateurs ne doivent en aucun cas se livrer sur internet à une activité illicite ou portant atteinte aux intérêts de l'entreprise.

Le téléchargement en tout ou partie de données numériques soumis aux droits d'auteurs ou à la loi du copyright est strictement interdit.
L'utilisateur s'engage à ne pas utiliser cet accès à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin, tels que des textes, images, photographies, œuvres musicales, œuvres audiovisuelles, logiciels et jeux vidéo, sans autorisation expresse et préalable. L'utilisation d'un logiciel de partage n'est pas autorisé, sauf accord de la Direction.

Le stockage sur le réseau de données à caractère non professionnel téléchargées sur internet est interdit.
Tout abonnement payant à un site web ou un service doit faire l'objet d'une autorisation préalable.
La Direction se réserve le droit pour éviter les abus de contrôler les connexions entrantes et sortantes et les accès aux sites les plus visités.

7. Reseaux Sociaux

Les utilisateurs ont accès à des réseaux sociaux professionnels (Glassdoor, Viadeo, LinkedIn...) et s'engagent à y respecter les règles suivantes:

- Seul est autorisé un accès à titre professionnel, sur autorisation expresse de la Direction;
- L'utilisateur ayant accès aux comptes de l'entreprise sur ces réseaux en est l'administrateur. Il est de sa responsabilité de s'occuper de leur maintenance et d'utiliser les paramètres de confidentialité de manière stricte ;
- Chaque utilisateur est responsable de ses propos, des liens ou photos qu'il poste. Aucune grossièreté, aucun propos insultant ou discriminatoire, ou dénigrant à l'encontre de l'entreprise ne saurait être tolérés ;
- Il est interdit de poster sur les réseaux sociaux des informations de nature confidentielle (exemples : échantillon de codes, rapports d'incident, données financières ou personnelles) ;
- Chaque utilisateur doit se conformer aux principes et à l'éthique de l'entreprise ;

La Direction se réserve le droit de contrôler l'utilisation qui est faite de réseaux sociaux et la nature des propos tenus par les utilisateurs.

Paraphe RA

8. TELEPHONE

L'utilisation des téléphones fixes est réservée à des fins professionnelles. Néanmoins un usage ponctuel du téléphone pour des communications personnelles locales est toléré à condition qu'il reste raisonnable en terme de durée et/ou de quantités d'appels et que cela n'entrave pas l'activité professionnelle. Les surcoûts entrainés par l'utilisation de la téléphonie à titre personnel tels appels et ou connections internets à des numéros surtaxés, et/ou depuis ou à destination de l'étranger devront être remboursés par les utilisateurs concernés.

Il est rappelé que l'envoi de SMS profesionnel quelque soit le support utilisé (mobile pro ou personnel) engage la responsabilité de l'émetteur au même titre que l'envoi d'un courriel. Il est donc soumis aux mêmes règles que rappelées plus haut.

La Direction se réserve le droit de procéder à des contrôles sur les appels émis ou reçus sur les téléphones à usage professionnel pour surveiller le volume d'activités et détecter des dysfonctionnement .

9. CONFIDENTIALITE

Les utilisateurs s'engagent à respecter une obligation générale et permanente de confidentialité et de discrétion à l'égard des informations et documents disponibles dans le système d'information.

Ainsi tout utilisateur s'engage :

- à ne transmettre aucune information confidentielle sans autorisation préalable ;
- à veiller à ce que les tiers non autorisés n'aient pas connaissance d'une telle information ;
- à ne pas rechercher ni ouvrir un message qui ne lui est pas adressé sans l'autorisation de son destinataire, à l'exclusion du supérieur hiérarchique ;
- à ne pas utiliser, sans l'accord de l'utilisateur concerné, les ressources qui sont affectées à ce dernier ;
- d'une manière générale, à respecter les règles d'éthique professionnelle, de déontologie, les obligations de réserve et le secret professionnel.

10. ANALYSE ET CONTROLE DE L'UTILISATION DES RESSOURCES

Pour des nécessités de maintenance et de gestion technique, de contrôle à des fins statistiques, de traçabilité d'optimisation, de sécurité ou détection des abus, l'utilisation des ressources informatiques et des services internet ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect de la législation applicable et notamment de la loi sur l'informatique et des libertés.

Paraphe RA

En cas de dysfonctionnement un contrôle peut être opéré sur toute opération effectuée par un utilisateur sur tout outil ou support mis à sa disposition, sur le réseau ou la messagerie. Sauf risque ou évènement particulier, la direction ne peut ouvrir les fichiers ou messages identifiés comme personnels ou liés à la représentation du personnel ou syndicale qu'en présence de l'utilisateur ou celui-ci dument appelé et éventuellement en presence d'un représentant du personnel.

Les personnels en charge des opérations de contrôle sont soumis à une obligation de confidentialité. Ils ne peuvent donc divulguer les informations qu'ils sont amenées à connaître dans le cadre de leur fonction, en particulier lorsqu'elles sont couvertes par les secrets de correspondances ou relèvent de la vie privée de l'utilisateur, dès lors que ces informations ne remettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt du service.

11. CONTROLES AUTOMATISES

11.1. CONTROLES

Le système d'information et de communication utilise des outils de traçabilité permettant de déterminer les adresses URL et/ou adresses IP auxquelles l'utilisateur a accédé lors de sa connexion (« 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 :

- à l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications et suppressions 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 et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements, dans le respect des règles en vigueur.

Paraphe
RA

11.2. PROCEDURE DE CONTROLE MANUEL

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

11.3. DECHIFFREMENT SSL DES SITES HTTPS

L'entreprise, pour des raisons de sécurité, déchiffre les sites web en HTTPS et les fait par conséquent analyser par un antivirus spécialisé.
Conformément aux recommandations de la CNIL, les sites Internet catégorisés banque, assurance, caisse santé sont exclus du déchiffrement afin de limiter toute atteinte au respect de la vie privée des utilisateurs.

12. SANCTIONS

En cas de manquement constaté aux règles énoncées dans la présente charte, la direction se réserve la possibilité de limiter ou supprimer immédiatement, une partie ou la totalité des accès du contrevenant aux ressources informatiques.
De plus tout manquement aux obligations, règles et mesures décrites dans la présente charte est susceptible d'entrainer la responsabilité de l'utilisateur et de donner lieu à des sanctions disciplinaires dans les conditions prévues par le Règlement Intérieur de l'entreprise et par les dispositions légales. L'utilisation reconnue à des fins personnelles de certains services payant à travers le système de communication de l'entreprise donnera également lieu à remboursement de la part de l'utilisateur concerné.
Enfin, l'entreprise se reserve également le droit d'engager ou de faire engager des poursuites civiles et pénales indépendamment des sanctions mises en oeuvre.

13. INFORMATION DES UTILISATEURS

La présente charte est annexée au règlement intérieur de l'entreprise, et est remis à l'embauche de chaque collaborateur, et à l'arrivée de chaque sous-traitant.
Un exemplaire de la présente charte est également affiché dans l'entreprise.
Le service informatique est à la disposition des utilisateurs pour leur fournir toute information concernant l'utilisation du système d'information et de communication. Il informe les utilisateurs régulièrement sur l'évolution des limites techniques du système d'information et sur les menaces susceptibles de peser sur sa sécurité.
Des opérations de communication interne et de formation sont organisées, de manière régulière, afin d'informer les utilisateurs sur les pratiques d'utilisation du système d'information et de communication recommandées.

Paraphe
RA

Chaque utilisateur doit s'informer sur les techniques de sécurité et veiller à maintenir son niveau de connaissance en fonction de l'évolution technologique et participer aux formations organisées.

14. REVISION DE LA CHARTE

La Charte sera régulièrement mise à jour et pourra faire l'objet d'adaptations spécifiques en fonction des catégories d'utilisateurs concernés en respect de la procédure de révision.

15. ENTREE EN VIGUEUR

La présente charte informatique entre en application le 01/01/2020. Elle a été soumise pour avis aux institutions représentatives du personnel (CSE), adressée en deux exemplaires à l'Inspecteur du travail puis envoyée en deux exemplaires au secrétariat-greffe du Conseil de Prud'hommes.

Fait à Nanterre, le 31/12/2019.

Paraphe RA