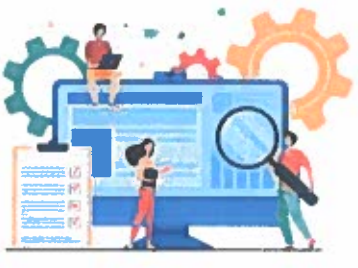
SPIN

Charte Informatique



1. GENERALITE

1.1 OBJET

L'entreprise met en œuvre un système d'information et de communication nécessaire à son activité, comprenant notamment un réseau informatique et téléphonique, ainsi que des outils mobiles.

La présente charte d'utilisation des moyens informatiques et de communications électroniques manifeste la volonté de l'entreprise d'assurer un développement harmonieux et sécurisé de l'accès et de l'utilisation des moyens informatiques et de communications électroniques.

La charte a pour finalité de contribuer à la préservation de la sécurité du système d'information de l'entreprise et fait de l'utilisateur un acteur essentiel à la réalisation de cet objectif. Elle formalise les règles de déontologie et de sécurité que l'utilisateur s'engage à respecter, en contrepartie de la mise à disposition par l'employeur des moyens informatiques et de communications électroniques. Elle définit aussi les moyens de contrôle et de surveillance de cette utilisation. Elle ne remplace en aucun cas les lois en vigueur que chacun est censé connaître.

1.2 APPLICATION

Elle entre en vigueur le 28/01/2022.

La charte est remise lors de l'embauche ou de l'entrée de l'utilisateur au sein de l'entreprise.

Elle est également affichée sur le panneau d'information et sur l'intranet de l'entreprise.

La charte s'applique à toutes les personnes autorisées à accéder ou à utiliser les moyens informatiques et de communications électroniques de l'entreprise et ce, quel que soit leur statut (notamment collaborateur, personnel intérimaire, stagiaire, apprentis, visiteurs occasionnels, etc.).

La charte s'applique à toutes les ressources mises à disposition de l'utilisateur par l'entreprise au jour de l'entrée en vigueur de la charte ou postérieurement, telles que celles désignées ci-dessous, et au(x) matériel(s) personnel(s) des utilisateurs connecté(s) au réseau de l'entreprise ou contenant des informations à caractère professionnel concernant l'entreprise.

- Un ordinateur de bureau ou un ordinateur portable
- Un téléphone fixe et/ou un téléphone portable
- Un fax
- Des photocopieurs et imprimantes
- Une tablette
- La messagerie électronique qui permet d'échanger entre deux ou plusieurs personnes, des messages auxquels peuvent être joints des fichiers de données ; l'accès est possible sur le lieu de travail et à distance
- Un réseau informatique comprenant éventuellement des serveurs de fichiers et le disque dur du poste de travail sur lesquels des espaces sont réservés à titre individuel ou collectif aux utilisateurs afin de stocker des informations ; l'accès aux serveurs de fichiers est possible sur le lieu de travail ou à distance sous réserve d'une validation conjointe de la direction et du service informatique
- Des fichiers, données et bases de données
- Un accès à internet et à l'intranet
- Des logiciels ayant pour objet exclusif de permettre à l'utilisateur d'exercer son activité professionnelle (exemple : Powerpoint, Outlook, Excel)
- Des outils collaboratifs.

Les salariés veillent à faire accepter les règles posées dans la charte à toute personne à laquelle ils permettraient d'accéder aux moyens informatiques et de communications électroniques.

La charte s'applique à tous les usages, qu'ils aient lieu ou non dans les locaux de l'entreprise.

Enfin, les règles encadrant l'utilisation et la diffusion d'informations confidentielles s'étendent à tous les moyens de communication, y compris la parole ou les documents papier.

2. OBLIGATIONS LEGALES

Il est rappelé que nul ne saurait se soustraire à la réglementation applicable, y compris dans le domaine de la sécurité informatique. Ainsi, l'utilisation des ressources informatiques par l'utilisateur doit être conforme à la législation en vigueur et notamment à :

- La législation relative à la fraude informatique
- La législation relative au secret des correspondances
- La législation relative à la propriété intellectuelle
- La loi du 04 août 1994 relative à l'emploi de la langue française
- La législation applicable en matière de cryptologie
- La réglementation relative à la protection des données à caractères personnelles, entre autres le règlement n° 2016/679, dit règlement général sur la protection des données et la loi du 6 janvier 1978 dite "informatique et liberté"
- La réglementation relative aux systèmes de traitement automatisé de données.

A titre d'exemple, sont ainsi notamment interdites et pénalement sanctionnées :

- L'atteinte à la vie privée d'autrui
- La diffamation et l'injure
- La provocation de mineurs à commettre des actes illicites ou dangereux, le fait de favoriser la corruption d'un mineur, l'exploitation à caractère pornographique de l'image d'un mineur, la diffusion de messages à caractère violent ou pornographique susceptibles d'être perçus par un mineur
- L'incitation à la consommation de substances interdites
- La provocation aux crimes et délits et la provocation au suicide, la provocation à la discrimination, à la haine notamment raciale, ou à la violence
- L'apologie des crimes, notamment meurtre, viol, crime de guerre et crime contre l'humanité ; la négation de crimes contre l'humanité
- La contrefaçon de marque
- La reproduction, représentation ou diffusion d'une œuvre de l'esprit (par exemple: extrait musical, photographie, extrait littéraire, ...) ou d'une prestation de droits voisins (par exemple interprétation d'une œuvre musicale par un artiste, phonogramme, vidéogramme, programme d'une entreprise de communication audiovisuelle) en violation des droits de l'auteur, du titulaire de droits voisins et/ou du titulaire des droits de propriété intellectuelle.

3. BONNE CONDUITE

Il est interdit de faire usage des moyens informatiques à des fins personnelles lucratives et/ou liées à des jeux de hasard, sauf autorisation expresse de la direction.

L'utilisateur 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.

L'utilisateur est informé et reconnait que des échanges électroniques peuvent constituer des preuves et former un contrat (c'est-à-dire constituer un engagement notamment au nom de l'entreprise).

Par conséquent, il doit être vigilant sur la nature des messages qu'il envoie et reçoit.

4. RESPONSABILITE SOCIALE ET ENVIRONNEMENTALE

Les outils informatiques et de communication, leur usage et notamment les services de messagerie électronique ont des impacts sur l'environnement.

L'objectif de l'entreprise est de favoriser et de développer un comportement responsable pour réduire son impact environnemental.

Aussi, l'entreprise recommande d'adopter des pratiques permettant de limiter l'impact environnemental :

- Préserver les équipements mis à disposition pour favoriser leur longévité et réduire la fréquence de leur remplacement
- Limiter la consommation d'énergie en ne laissant pas les équipements allumés ou en veille en permanence
- Désactiver les fonctions telles que le Wifi, le Bluetooth lorsqu'elles ne sont pas utilisées
- Optimiser les impressions (recto-verso, noir et blanc, etc.)
- Privilégier les échanges en optimisant la quantité de données transmises notamment en évitant les signatures électroniques comprenant des images, en compressant les fichiers ou en utilisant un lien de partage plutôt que l'envoi d'un fichier
- Utiliser les favoris pour accéder à un site internet régulièrement plutôt que lancer une requête à chaque fois
- Nettoyer régulièrement sa messagerie.

5. IMAGE DE L'ENTREPRISE

Il est rappelé qu'à l'occasion de chaque utilisation du réseau internet (serveur web, messagerie électronique, réseaux sociaux, etc.), l'utilisateur véhicule l'image de l'entreprise. L'utilisateur n'émettra pas d'opinions personnelles étrangères à son activité professionnelle susceptibles de porter préjudice à l'entreprise.

Notamment, l'utilisateur étant sur son lieu de travail ne doit pas consulter, envoyer et/ou stocker des contenus à caractères pornographiques, violents ou véhiculant des idées politiques ou faisant du prosélytisme.

Toute communication sur les réseaux sociaux à caractère professionnel ou privé (Viadéo, Linkedin, Facebook, Twitter, etc.) au nom de l'entreprise ou relative à l'image de l'entreprise est interdite sauf accord exprès de la direction.

6. CONFIDENTIALITE

Il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, y compris dans des fichiers non protégés. Cette règle s'applique de la même façon aux répertoires réseaux et aux courriers dont l'utilisateur ne serait pas destinataire.

Dans le cadre de ses obligations contractuelles, l'utilisateur est tenu à la plus grande discrétion quant aux informations obtenues dans le cadre professionnel. De nombreuses informations confidentielles ou dites sensibles peuvent être échangées et confiées à l'utilisateur. Ce dernier est responsable pour ce qui le concerne du respect du secret professionnel et de la confidentialité des informations qu'il est amené à détenir, consulter ou utiliser. Il est dans l'obligation de porter la plus grande attention aux conditions de sécurité dans lesquelles les échanges s'effectuent notamment par messagerie. Lors de l'envoi de données sensibles et/ou confidentielles et/ou à caractère personnel via un réseau, l'utilisateur s'engage à chiffrer les pièces sensibles à transmettre si cette transmission utilise la messagerie électronique et/ou utiliser un protocole garantissant la confidentialité et l'authentification du serveur destinataire pour les transferts de fichiers. Les clés de chiffrement, mot de passe etc. devront être transmis via un canal distinct (par exemple : envoi du fichier chiffré par email et communication du mot de passe par téléphone ou SMS).

Par ailleurs, les utilisateurs veilleront à respecter les éléments suivants :

- Tout document confidentiel et/ou comportant des informations sensibles devra comprendre la mention « CONFIDENTIEL » sur chaque page.
- Tout courriel confidentiel et/ou comportant des informations sensibles devra comprendre la mention « CONFIDENTIEL » en objet.

Lorsqu'un document est considéré comme confidentiel ou lorsque le terme « confidentiel » est apposé sur un document professionnel, l'utilisateur devra veiller à le conserver dans un espace de stockage non accessible aux autres utilisateurs.

Les informations professionnelles devant être protégées se présentent notamment et de manière non-exhaustive sous la forme de :

- L'organisation, les activités, les études (administratives, commerciales ou financières) et les résultats financiers de l'entreprise et de ses clients ou prospects
- Les techniques, savoir-faire, méthodes, projets, logiciels, codes informatiques, etc.
- Les données personnelles sensibles appartenant à une personne ou un groupe de collaborateurs
- Ou tous autres éléments qui de par leur nature relèvent d'un caractère confidentiel.

Ces informations constituant le patrimoine immatériel de l'entreprise, il convient de les protéger d'une manière spécifique, notamment en s'assurant que l'utilisateur :

- N'envoie ou ne soumet pas d'informations confidentielles, sous toute forme et quelle qu'en soit la raison, à toute personne non habilitée à en avoir connaissance
- Ne laisse pas sans surveillance tout type de support contenant des informations confidentielles
- Conserve de manière sécurisée les documents papiers confidentiels
- Verrouille sa session quand il n'est pas à côté de son ordinateur ou de son téléphone portable.

En cas d'impression de documents confidentiels, l'utilisateur devra veiller à aller chercher immédiatement les documents à la sortie de l'imprimante.

L'utilisateur doit être conscient que le respect des dispositions ci-dessus et contenues dans la présente Charte ne se limite pas à l'utilisation de moyens informatiques, mais s'étend également à l'usage de tout moyen de communication (y compris orale) et en tous lieux. Il veillera notamment à bien raccrocher son téléphone à la fin d'une communication téléphonique et à ne pas laisser, le cas échéant, de pont téléphonique ouvert en cas de conférence téléphonique créée.

L'utilisateur s'engage notamment à être vigilant lorsqu'il se trouve dans un lieu public (par exemple au restaurant ou dans les transports en commun), lorsqu'il a une conversation professionnelle, ou qu'il consulte un document confidentiel.

7. DROIT A LA DECONNEXION

Il est important de faire bon usage des outils informatiques en vue d'un nécessaire respect des temps de repos et de congé ainsi que l'équilibre entre la vie privée et familiale et la vie professionnelle.

7.1 LUTTE CONTRE LE STRESS LIE A L'UTILISATION DES MOYENS INFORMATIQUES ET DE COMMUNICATIONS ELECTRONIQUES

Afin d'éviter le stress lié à l'utilisation des moyens informatiques et de communications électroniques, il est recommandé à tous les utilisateurs de :

- S'interroger sur le moment opportun pour envoyer un courriel/SMS ou appeler un collaborateur sur son téléphone professionnel (pendant les horaires de travail)
- Ne pas solliciter de réponse immédiate si cela n'est pas nécessaire
- Privilégier l'envoi des courriels pendant les horaires de travail y compris lorsqu'un courriel a été rédigé en dehors des horaires de travail.

7.2 DROIT A LA DECONNEXION EN DEHORS DU TEMPS DE TRAVAIL EFFECTIF

Les périodes de repos, congés et suspension du contrat de travail doivent être respectées par l'ensemble des acteurs de l'entreprise.

Les responsables hiérarchiques ne peuvent pas contacter leurs subordonnées sauf astreinte ou urgence avérée, en dehors de leurs horaires de travail.

En dehors de son temps de travail et des temps d'astreinte, le salarié n'est pas tenu de prendre connaissance des courriels, appels et messages téléphoniques qui lui sont adressés.

8. ACCES A L'ORDINATEUR DE L'UTILISATEUR EN SON ABSENCE

En cas d'absence prolongée, l'entreprise peut avoir besoin de consulter les fichiers et/ou la messagerie de l'utilisateur afin d'assurer la continuité du service.

Dans ce cadre, le responsable pourra décider :

- De prévoir le principe de la suspension de la messagerie en cas d'absence prolongée de l'utilisateur et la mise en place d'un message automatique envoyé à partir de la boite mail de l'utilisateur afin de donner les noms des personnes à contacter en l'absence du salarié, permettant ainsi d'assurer la continuité du service
- De transférer automatiquement les emails du salarié sur une autre messagerie.

Cependant, le répertoire personnel tel que prévue à l'article 13.3, les fichiers y figurant et les messages identifiés comme personnels dans leur objet ne pourront être ouverts.

9. UTILISATION DES MOYENS INFORMATIQUES ET DE COMMUNICATIONS ELECTRONIQUES A TITRE PERSONNEL

L'utilisation des moyens informatiques et de communications électroniques à des fins non professionnelles, pour répondre à des obligations urgentes, est tolérée lorsqu'elle s'effectue dans les conditions de la présente charte et notamment des articles 13, 15 et 16.

Cette utilisation doit être exceptionnelle, respectueuse, raisonnable et loyale. Un tel usage ne doit pas perturber le bon fonctionnement du service et créer ou risquer de créer des dysfonctionnements, saturation, atteintes à la sécurité ou détournement des moyens mis à disposition. Par ailleurs, cette utilisation ne saurait être abusive par sa fréquence ou porter préjudice à la productivité et à la qualité du travail fourni. L'entreprise se réserve le droit de limiter ou de suspendre cette tolérance en cas d'abus.

Les messages électroniques échangés sont, en tout état de cause, émis et reçus sous la seule responsabilité de l'utilisateur qui dégage l'entreprise de toute responsabilité.

Toute utilisation à des fins lucratives est interdite.

10.ACCES AUX RESSOURCES INFORMATIQUES

De manière générale, l'utilisateur doit prendre toutes les mesures pour limiter les accès frauduleux aux ressources informatiques mises à sa disposition.

Chaque outil informatique (poste de travail, ordinateur portable, téléphone mobile etc.) doit être protégé par un mot de passe.

10.1 CONFIDENTIALITE DES IDENTIFIANTS TRANSMIS PAR L'ENTREPRISE

Les ressources informatiques sont protégées par un mot de passe et un login qui sont attribués et/ou choisi par l'utilisateur.

Le mot de passe choisi par l'utilisateur doit être individuel, difficile à deviner et rester secret.

Afin de conserver et de gérer des mots de passe longs, complexes et tous différents, l'utilisateur peut recourir à un gestionnaire de mots de passe conformément aux préconisations fournies par le service informatique.

L'utilisateur ne devra pas, pour des raisons évidentes de sécurité :

- Stocker ses mots de passe dans un fichier en clair, sur un papier ou dans un lien facilement accessible par d'autres personnes
- Enregistrer ses mots de passe dans son navigateur
- Utiliser des mots de passe ayant un lien avec soi (nom, date de naissance, etc.), le mot de passe devant faire preuve d'originalité
- Utiliser le même mot de passe pour des accès différents
- Conserver les mots de passe par défaut
- S'envoyer par email ses propres mots de passe.

Le mot de passe devra être régulièrement renouvelé par l'utilisateur.

L'utilisateur est responsable de la protection de ses identifiants et doit choisir des mots de passe sûrs.

Ces identifiants sont strictement confidentiels et personnels. Ils ne peuvent en aucun cas être délégués, communiqués ou cédés, même temporairement, à un tiers même intra-service. Toutefois, si un utilisateur absent détient sur son poste des informations indispensables à la poursuite de l'activité, l'employeur peut exiger la communication de ses codes si l'administrateur réseau n'est pas en mesure de fournir l'accès au poste.

L'utilisateur s'engage à informer immédiatement le service informatique de toute perte, tentative de violation ou anomalie relative à une utilisation de ses Identifiants.

10.2 RESPECT DES DROITS D'ACCES OCTROYES PAR L'ENTREPRISE

L'entreprise accorde à titre individuel et nominatif à l'utilisateur, des droits d'accès à certains logiciels, outils et dossiers de travail disponibles sur le réseau ainsi que sur les postes informatiques. Ces droits peuvent différer selon la fonction que l'utilisateur exerce dans l'entreprise afin de s'adapter aux besoins réels de l'utilisateur pour l'accomplissement de sa mission de travail.

Les droits d'accès sont personnels, intransmissibles, inaliénables et temporaires. Ils ne peuvent en aucun cas être délégués, communiqués ou cédés, même temporairement, à un tiers. Il est strictement interdit de tenter de s'octroyer des droits d'accès supplémentaires ou d'accéder à des ressources de l'entreprise sans avoir les droits d'accès requis.

L'utilisateur ne doit pas utiliser ou essayer d'utiliser des comptes autres que le sien ou de masquer sa véritable identité.

L'utilisateur s'engage à ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux, notamment à travers des matériels dont il a l'usage. Notamment, l'utilisateur doit systématiquement se déconnecter et verrouiller son poste de travail, son téléphone mobile ou tout autre outil informatique en libre-service ou non avant de s'en séparer, afin de ne pas laisser des ressources ou services accessibles à tous.

En cas d'urgence ou pour des raisons liées à la protection des données ou outils de l'entreprise, au besoin de maintenir un niveau de qualité de service, l'entreprise peut procéder à la destruction ou réinitialiser les codes d'accès d'un utilisateur.

10.3 MODIFICATION, RETRAIT OU SUSPENSION DES DROITS D'ACCES

L'entreprise se réserve le droit de supprimer, restreindre ou rajouter des droits d'accès à des machines, des interfaces ou autre, selon la compétence de l'utilisateur ou du service auquel ce dernier est rattaché.

Les droits d'accès peuvent être retirés à tout moment. En tout état de cause, tout droit d'accès prend fin lors de la cessation, même provisoire, de l'activité professionnelle qui l'a justifié.

Toute violation des termes de la charte informatique peut donner lieu à la suspension immédiate des droits d'accès par l'entreprise et ce, sans exclure d'éventuelles sanctions disciplinaires et/ou pénales.

11.MAINTENANCE DES RESSOURCES INFORMATIQUES

Les opérations de maintenance des moyens informatiques et de communications électroniques sont nécessaires afin d'assurer le bon fonctionnement et la sécurité des systèmes d'information. Sauf indication contraire de la part du service informatique, l'utilisateur doit accepter et ne peut pas s'opposer aux mises à jour de ses moyens informatiques et de communications électroniques. Les opérations de maintenance peuvent également nécessiter l'intervention d'une personne habilitée sur site ou sous la forme d'une « prise de main à distance ». La personne habilitée est la personne désignée à cet effet par l'employeur.

Le service informatique peut interrompre l'accès aux moyens informatiques et de communications électroniques, notamment pour des raisons de maintenance et/ou de mise à niveau, sans être tenu pour responsable des conséquences de ces interruptions aussi bien pour l'utilisateur que pour tous tiers. Toutefois, il s'engage dans la mesure du possible à faire connaître aux utilisateurs, par avance, via un courrier électronique, les plages d'interruptions de service lorsque celles-ci correspondent à des maintenances ou des interventions programmées.

Par défaut, tous les contenus présents sur les outils informatiques ont un caractère professionnel et peuvent donc être consultés et utilisés par l'employeur, y compris en dehors de la présence de l'utilisateur. Ainsi, la personne habilitée peut être amenée à accéder aux contenus des outils informatiques. Seuls les courriels précisant « *Personnel* » dans leur objet ou stockés dans un répertoire intitulé « *Personnel* » seront considérés comme étant des correspondances non-professionnelles. Les fichiers identifiés comme personnels dans leur nom pourront être consultés en présence de l'utilisateur ou après appel infructueux.

12.CONSERVATION DES DONNEES

L'utilisateur doit régulièrement supprimer ses données devenues inutiles et archiver les données anciennes à conserver, si besoin avec l'aide du service informatique.

Les messages électroniques sont conservés sur le serveur de messagerie à l'image de ce qui existe sur le poste de l'utilisateur. Il n'existe pas à ce jour d'archivage intégral de tout mail entrant et sortant.

Par principe, la messagerie n'est pas un lieu d'archivage. Il appartient à chaque utilisateur d'assurer sa propre gestion et conservation des données.

13.UTILISATION DES SERVEURS DE FICHIERS ET DU DISQUE DUR

13.1 REGLE D'UTILISATION DES SERVEURS DE FICHIERS ET DU DISQUE DUR

Les serveurs de fichiers sont des espaces communs de stockage d'informations et le disque dur est un espace individuel de stockage directement sur l'ordinateur de l'utilisateur.

A l'exception de l'espace qui est proposé à l'utilisateur dans les conditions de l'article 9 de la charte, les éléments informatiques stockés dans ces espaces doivent être strictement professionnels et en regard direct avec l'activité professionnelle de l'utilisateur.

13.2 RESPECT DES OBLIGATIONS LEGALES ET DES REGLES GENERALES DE BONNE CONDUITE

L'utilisateur devra, pour toutes opérations qu'il effectue sur les ressources informatiques, respecter la législation en vigueur ainsi que les règles de bonne conduite, telles qu'indiquées aux articles 2 et 3 de la charte informatique.

13.3 UTILISATON DES SERVEURS DE FICHIERS ET DU DISQUE DUR A DES FINS PERSONNELLES

Tout fichier ou dossier créé par l'utilisateur avec les ressources informatiques de l'entreprise est réputé appartenir à l'entreprise. L'employeur pourra donc y avoir accès.

Cependant, l'entreprise tolère que l'utilisateur crée sur son poste de travail un dossier dans lequel sont uniquement enregistrées des données relatives à sa vie privée, personnelle ou familiale. En aucune façon, ce dossier ne doit contenir des informations professionnelles. Le stockage de ces données n'est toléré qu'à la condition formelle de sa conformité avec les lois et règlements (bonnes mœurs, propriété intellectuelle, etc.) et qu'il n'interfère pas en termes de capacité et de fonctionnement sur les moyens informatiques. Afin d'éviter toute ambiguïté sur la nature de ce dossier, celui-ci devra être intitulé « *personnel* » ou « *perso* ».

Toutes données sans lien avec l'activité professionnelle de l'utilisateur peuvent être supprimées par l'entreprise si elles se situent hors du dossier personnel.

L'utilisateur reconnait que tous les contenus présents sur les outils informatiques ont un caractère professionnel et peuvent donc être consultés et utilisés par l'employeur, y compris en dehors de la présence de l'utilisateur. Seul le dossier identifié comme personnel dans son nom ne pourra être consulté qu'en présence de l'utilisateur ou après appel infructueux ainsi qu'en cas de risque ou évènement particulier.

13.4 CLOTURE DU COMPTE

Lorsqu'un utilisateur quitte définitivement l'entreprise, le service informatique supprime son compte dans un délai de 1 mois sans nécessairement effectuer de sauvegarde dès réception d'une notification de la sortie du salarié. L'utilisateur devra donc veiller à récupérer par ses propres moyens ses données personnelles avant de quitter l'entreprise.

En outre, au jour de la remise du matériel, il lui sera demandé :

- D'attester de la suppression de l'ensemble des éléments identifiés comme personnel ou privé présents dans son ordinateur,
- D'avoir transféré à son supérieur/ son équipe l'ensemble des dossiers/documents et plus généralement tous les éléments nécessaires à la continuité du service et de l'entreprise SPIN.

En cas de départ de la société, l'utilisateur ne peut en aucun cas, réinitialiser lui-même les outils informatiques, ordinateur, téléphone mis à disposition par la société ainsi que supprimer les données figurant dans ses dossiers sauf les données figurant dans le dossier identifié comme personnel.

14.UTILISATION DES LOGICIELS

L'utilisateur ne peut obtenir qu'après autorisation de son responsable hiérarchique et/ou du service informatique, l'installation d'un logiciel ou d'un plug-in, même gratuit. Il ne doit pas installer de logiciel sans cette autorisation.

Il est strictement interdit à tout utilisateur de faire des copies de logiciels commerciaux pour quelque usage que ce soit.

15.UTILISATION D'INTERNET

15.1 REGLE D'UTILISATION D'INTERNET

Pendant son temps de travail, l'utilisateur ne pourra consulter des sites internet que pour ses besoins professionnels. Principalement pour des raisons de sécurité et de disponibilité des moyens informatiques et de communications électroniques, l'entreprise peut restreindre l'accès à Internet.

Il est interdit à l'utilisateur de se connecter, via les moyens informatiques et de communications électroniques, à des sites internet dont le contenu est contraire à l'ordre public, aux bonnes mœurs ou à l'image de marque de l'entreprise, ainsi qu'à ceux pouvant comporter un risque pour la sécurité des systèmes d'information et outils de l'entreprise.

Pendant son temps de travail, l'utilisateur veille à ce que les pages web apparues par « pop up « n'ayant pas de lien avec son activité professionnelle soient complètement fermées et n'apparaissent pas de ce fait sur la barre d'outils de son poste de travail.

L'entreprise a également mis en place diverses mesures permettant d'assurer la sécurité du réseau local et des postes de travail (pare-feu, anti-virus etc.). L'utilisateur s'engage à ne pas les désactiver, interférer avec ces mesures, notamment en les désinstallant ou en bloquant leurs mises à jour.

L'utilisateur devra être vigilant dans l'usage qu'il fait d'internet et ne devra pas contourner, sauf autorisation, les protections mises en place par l'entreprise.

L'utilisateur ne devra pas se connecter à des réseaux sans fil inconnus et qui ne sont pas de confiance avec ses outils informatiques et de communications électroniques, y compris les ordinateurs portables et téléphones mobiles.

15.2 RESPECT DES OBLIGATIONS LEGALES ET DES REGLES GENERALES DE BONNE CONDUITE

L'utilisateur devra, lorsqu'il utilise internet, respecter la législation en vigueur ainsi que les règles de bonne conduite, telles qu'indiquées à l'article 3 de la charte informatique.

L'utilisateur est informé que le service informatique peut enregistrer son activité sur internet et que ces traces pourront être exploitées à des fins de preuves, statistiques, contrôle et vérification dans les limites prévues par la loi.

16.UTILISATION DE LA MESSAGERIE ELECTRONIQUE

Chaque utilisateur dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique attribuée par le service informatique. Les règles ci-dessous s'appliquent quel que soit le moyen utilisé par l'utilisateur pour consulter cette messagerie.

16.1 REGLE D'UTILISATION DE LA MESSAGERIE ELECTRONIQUE

L'utilisateur s'engage à ne pas effectuer des opérations pouvant nuire au fonctionnement de la messagerie, à savoir :

- Ne pas introduire de virus
- Limiter l'envoi de message uniquement aux destinataires réellement intéressés, pour éviter la saturation du réseau et des serveurs et ne pas obliger les destinataires à lire des messages sans intérêt pour eux
- Ne pas procéder à des envois massifs de courriers
- Prévenir le risque de saturation des boîtes aux lettres et des serveurs en évitant de joindre à un même message des documents trop volumineux et en utilisant chaque fois que possible des outils de compression
- Nettoyer régulièrement sa boîte aux lettres en supprimant les courriers inutiles afin de prévenir le risque évoqué ci-dessus de saturation des boîtes aux lettres et des serveurs.

16.2 RESPECT DES OBLIGATIONS LEGALES ET DES REGLES GENERALES DE BONNE CONDUITE

L'utilisateur devra respecter la législation en vigueur et les règles de bonne conduite concernant les textes, images, vidéos et pièces jointes en tout genre, présents dans les courriers électroniques.

Les courriers électroniques ne doivent pas comporter d'éléments illicites, tels que des propos diffamatoires, injurieux, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire.

Il est rappelé à l'utilisateur que les courriers électroniques peuvent être constitutifs de preuves et sont engageant pour l'entreprise et l'utilisateur au même titre qu'un écrit papier.

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

En cas d'absence, l'utilisateur est invité à mettre en place une réponse automatique.

16.3 LIMITATION DE LA TAILLE DE LA MESSAGERIE ELECTRONIQUE

Afin de faciliter la gestion des espaces disques et prévenir la saturation des serveurs, le compte de messagerie électronique de l'utilisateur est limité en taille. L'utilisateur est personnellement responsable de cet espace disque et doit veiller à ce que sa taille reste toujours inférieure à la taille limite. Dans le cas où cet espace serait saturé, des messages indiqueront à l'utilisateur que les limites sont atteintes et qu'il doit effectuer des suppressions ou des archivages.

17.TELEPHONIE

Pour les besoins de leur activité professionnelle, l'utilisateur peut disposer d'un poste fixe et d'un terminal mobile. Il est rappelé que les dispositions de la présente charte sont également applicables à ces appareils, en particulier celles concernant l'utilisation d'internet, de la messagerie électronique et des logiciels.

Il est également rappelé que l'envoi de SMS est réservé aux communications professionnelles et qu'il engage la responsabilité de l'émetteur au même titre que l'envoi d'un courriel. Il est donc soumis aux mêmes règles que celles concernant l'utilisation de la messagerie électronique. Les connexions depuis l'étranger sont strictement interdites sauf autorisation exceptionnelle de la hiérarchie.

L'utilisation à des fins personnelles du téléphone, fixe ou mobile, est tolérée, à condition qu'elle reste dans des limites raisonnables en termes de temps passé et de quantité d'appels. Cependant, l'utilisateur ne pourra appeler des numéros surtaxés sans l'accord de la direction.

L'utilisateur est informé que la direction pourra avoir accès à ses activités téléphoniques, aussi bien sur les postes fixes que sur les mobiles. Ces traces seront exploitées à des fins statistiques, de contrôle et de vérification dans les limites prévues par la loi. Toutefois, seule la direction pourra avoir accès aux factures et numéros détaillés, permettant d'identifier les interlocuteurs d'un utilisateur, lorsque cela résulte d'une obligation légale, d'une réquisition judiciaire et en cas de nécessité pour la constatation, l'exercice ou la défense de droits en justice.

18.ACCES AU SYSTEME D'INFORMATION EN SITUATION DE MOBILITE

Lors des déplacements professionnels, l'utilisateur doit utiliser les connexions au système de l'entreprise auxquelles il a accès par connexion internet. Il doit veiller aux conditions dans lesquelles il accède en évitant notamment les accès depuis les lieux publics (clients, fournisseurs, etc.), pour privilégier le partage de connexion avec son téléphone mobile.

En cas d'accès via un autre type de poste que celui remis par l'entreprise, l'utilisateur doit veiller à ne pas accéder à des informations ou documents confidentiels sur des postes dont la sécurité est incertaine.

D'une façon générale et quel que soit le lieu de connexion, l'utilisateur de matériels mobiles (ordinateur, terminal mobile) et de supports informatiques (clé USB,...) doit veiller à la sécurité du matériel et des données qu'il contient.

L'utilisateur doit avoir un niveau de surveillance et de confidentialité renforcé.

Il doit :

- Adopter une attitude de prudence et de réserve au regard des informations et des ressources du système d'information de l'entreprise qu'il pourrait être amené à manipuler ou à échanger
- Veiller à ce que des tiers non autorisés ne puissent accéder à ces moyens, les utiliser ou accéder à leur contenu
- Veiller à ce qu'il soit authentifié « normalement » et conformément aux règles communiquées par le service informatique pour atteindre les services internes
- Utiliser un filtre écran lorsqu'il travaille dans des zones publiques ou des transports en commun
- Laisser sur les espaces de stockage les documents qui ne sont pas indispensables à sa mission
- Avoir des copies de sauvegardes en lieu sûr des documents qu'il transporte en « mobilité »
- Prendre en compte les alertes ou phénomènes inhabituelles qui pourraient révéler une activité frauduleuse en cours
- Verrouiller son ordinateur et son terminal mobile lorsqu'ils ne sont pas utilisés.

L'utilisateur ne doit pas :

- Laisser son matériel sans surveillance. Un accès très temporaire à un terminal mobile peut suffire à sa compromission sans que l'utilisateur en ait conscience, même lorsqu'il est verrouillé
- Rapatrier des documents ou des informations externes par l'intermédiaire d'une clé USB ou de tout type de support assimilé (l'échange de fichiers, informations, documents externes doit se faire par l'intermédiaire d'un transfert sécurisé, courrier électronique ou plateforme d'échange de fichiers sécurisée et si possible interne).

En cas non seulement d'incident avéré mais également de doute, l'utilisateur doit immédiatement en aviser le service informatique de l'entreprise dans les plus brefs délais, à l'adresse adminsys@ifterritoires.fr , dans un courriel avec importance haute.

19.VOL/PERTE DES OUTILS MIS A DISPOSITION

L'utilisateur ne doit jamais laisser ses outils sans surveillance notamment en dehors de l'entreprise ou dans un véhicule. L'utilisateur devra conserver ses outils informatiques et fichiers avec lui lors de ses déplacements.

L'utilisateur disposant d'un ordinateur portable doit s'assurer que celui-ci est en permanence attaché à un support fixe, grâce au câble de sécurité fourni par l'entreprise.

Afin de réduire les impacts d'un éventuel vol ou d'une perte d'outil informatique nomades (téléphone portable, tablettes, PC portable...), l'utilisateur s'engage à limiter le stockage de données sur ses outils informatiques au strict nécessaire et à régulièrement sauvegarder ses données conformément aux dispositions de la charte informatique.

L'utilisateur s'engage également à éviter d'emporter des données sensibles lors de ses déplacements, pour privilégier la récupération des fichiers chiffrés sur son lieu de mission en accédant au réseau de l'entreprise avec une liaison sécurisée et/ou via des communications chiffrées et authentifiées telles que mises à disposition par le service informatique.

En cas d'utilisation d'un matériel informatique non fourni par l'entreprise, l'utilisateur s'engage à ne pas stocker, ni utiliser les mots de passe de ses outils informatiques.

L'utilisateur marque ses outils informatiques d'un signe distinctif au nom de l'entreprise avant ses déplacements afin de surveiller plus facilement son matériel et d'éviter les échanges frauduleux. La suppression du signe distinctif sur les équipements fournis par l'entreprise est interdite.

En cas de vol, perte, inspection ou saisie d'un outil informatique, l'utilisateur doit informer le service informatique via un courriel avec importance haute en mettant en copie son responsable hiérarchique.

20.RESPONSABILITE

20.1 RESPONSABILITE DE L'ENTREPRISE

Le service informatique est responsable de la mise en œuvre et du contrôle du bon fonctionnement des moyens informatiques et de communications électroniques.

Il prévoit un plan de sécurité et de continuité du service, en particulier en cas de défaut matériel.

Il veille à l'application des règles de la présente charte. Il est assujetti à une obligation de confidentialité sur les informations qu'il est amené à connaître.

Afin de surveiller l'activité des moyens informatiques et de communications électroniques, le service informatique peut mettre en place des fichiers journaux (« logs ») et des traitements de données relatifs :

- A 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 ou le téléchargement de fichiers
- Aux appels téléphoniques émis ou reçus à partir des postes fixes ou mobiles pour surveiller le volume d'activités et détecter des dysfonctionnements.

Les fichiers journaux sont conservés 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.

Il est ainsi possible pour l'entreprise de contrôler l'activité et les échanges des utilisateurs.

Des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements, dans le respect des règles en vigueur.

Il est précisé que chaque utilisateur pourra avoir accès aux informations enregistrées lors de ces contrôles le concernant sur demande préalable à la direction. De plus, les fichiers journaux énumérés ci-dessus sont automatiquement détruits dans un délai maximum de 6 mois après leur enregistrement.

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. Le contrôle concernant un utilisateur peut porter sur les fichiers contenus sur le disque dur de l'ordinateur, sur un support de sauvegarde mis à sa disposition ou sur le réseau de l'entreprise, ou sur sa messagerie. Alors, sauf risque ou événement particulier.

20.2 RESPONSABILITE DE L'UTILISATEUR

Chaque utilisateur est responsable des moyens informatiques et de communications électroniques mis à sa disposition par l'entreprise et de l'utilisation qu'il fait du réseau de l'entreprise et des informations à caractère professionnel concernant l'entreprise et s'engage à ne pas y porter atteinte.

Ainsi, l'utilisateur ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède et doit faire preuve de prudence et de vigilance dans l'utilisation des moyens informatiques et de communications électroniques. Notamment, l'utilisateur ne doit pas contourner ou tenter de contourner les systèmes de sécurité mis en œuvre dans l'entreprise.

Les moyens informatiques et de communications électroniques mis à la disposition de l'utilisateur, sont exclusivement installés et configurés par le service compétent de l'entreprise. L'utilisateur s'interdit de modifier les équipements par ajout de logiciels ou matériels sans accord préalable du service informatique. Certaines

configurations et sites informatiques, peuvent être verrouillés par le service informatique.

Dans le cadre d'un besoin spécifique, l'utilisateur procède à une demande auprès de sa hiérarchie.

En particulier, l'utilisateur doit veiller à ne pas introduire de virus dans les ressources informatiques de l'entreprise. Pour ce faire, l'utilisateur ne doit notamment pas connecter de matériels informatiques autres que ceux mis à disposition par l'entreprise (tels que clés USB ou smartphones) aux équipements de l'entreprise (par exemple en rechargeant un smartphone par un câble USB relié à un ordinateur mis à disposition par l'entreprise).

Concernant les ordinateurs portables personnels, l'entreprise tolère qu'ils soient introduits dans les locaux aux conditions expresses et cumulatives suivantes :

- Ils doivent être allumés et utilisés exclusivement en dehors du temps de travail
- Ils ne doivent en aucun cas être connectés au(x) réseau(x) de l'entreprise

Tout travail de recherche risquant de conduire à une rupture de l'intégrité des systèmes, tel que l'introduction de logiciels parasites connus sous le nom générique de virus, ne pourra être accompli qu'avec l'autorisation du service informatique et dans le strict respect des règles qui auront alors été définies.

L'utilisateur ne peut lire, modifier, copier ou détruire, les données appartenant à l'entreprise si ces actions n'entrent pas expressément dans le cadre de sa mission de travail.

En cas d'incident de sécurité, anomalie ou événement inhabituel touchant aux systèmes d'information et de communication de l'entreprise, ou encore en cas de violation ou tentative de violation de l'intégrité des moyens informatiques et de communications électroniques, l'utilisateur s'engage à en informer immédiatement le service informatique par courriel avec importance haute, à l'adresse suivante guichet.sysinfo@ifterritoires.fr.

En cas d'anomalie, chaque utilisateur est responsable de la remontée d'information au service informatique qui effectuera le diagnostic de l'anomalie et la corrigera.

Enfin, chaque responsable hiérarchique est en charge de la bonne application de la présente charte au sein de ses équipes et de la remontée d'informations concernant une violation de celle-ci.

21.SANCTIONS

Tout manquement aux règles et mesures de sécurité figurant dans la présente charte engage la responsabilité personnelle de l'utilisateur, dès lors qu'il est prouvé que les faits fautifs lui sont personnellement imputables.

Par ailleurs, tout usage ou utilisation illicite de données personnelles par l'un des utilisateurs constituerait une violation de la réglementation en matière de protection des données personnelles serait passible de sanctions.

En cas d'urgence, l'entreprise et/ou le service informatique pourront également prendre la décision :

- De déconnecter un utilisateur, avec ou sans préavis selon la gravité de la situation
- D'isoler ou neutraliser toute donnée ou fichier manifestement en contradiction avec la présente charte ou qui mettrait en péril la sécurité des moyens informatiques.

A Paris, le 12 / 12 / 2023
Olivier RAUGEL, Président

SOCIETE DE PARTICIPATION
ET D'INVESTISSEMENT
DANS LE NUMERIQUE
14 RUE CAMBACERES
SAS AU CAPITAL DE 300€
SIRET 980 465 108 00010