Charte Informatique

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.

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.

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.

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 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.

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.

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 25 / 06 / 2024
Olivier RAUGEL, Président