

# CHARTE INFORMATIQUE

# SOMMAIRE

*PREAMBULE*

*CHAMP D'APPLICATION*

*PROTECTION DES DONNES PERSONNELLES*

## PARTIE 1 : UTILISATION DU SYSTEME D'INFORMATION

*ARTICLE 1. ACCES AU SYSTEME D'INFORMATION*

*ARTICLE 2. REGLES DE SECURITE DU SI*

*ARTICLE 3. RAPPEL DES PRINCIPES APPLICABLE EN CAS DE  
TRAITEMENT PORTANT SUR DES DONNEES PERSONNELLES*

*ARTICLE 4. INTERNET*

*ARTICLE 5 – COMMUNICATION SUR INTERNET / RESEAUX SOCIAUX*

*ARTICLE 6- MESSAGERIE PROFESSIONNELLE*

*ARTICLE 7. SERVICE INFORMATIQUE ET CONTRÔLE DES ACTIVITES.*

## PARTIE 2- CONDITIONS D'UTILISATION DES OUTILS INFORMATIQUES

*ARTICLE 8- REMISE DES OUTILS ET ACCES*

*ARTICLE 9. USAGE PROFESSIONNEL*

*ARTICLE 10. DROIT A LA DECONNEXION*

*ARTICLE 11. OUTILS PERSONNELS*

*ARTICLE 12. PROPRIETE INTELLECTUELLE*

*ARTICLE 13. SUSPENSION / DEPART DE L'UTILISATEUR*

*ARTICLE 14. RESPONSABILITES – SANCTIONS*

## ***PREAMBULE***

La société Sign IT met en place un système d'information et de communication nécessaire à l'exercice de l'activité. Elle met à disposition des utilisateurs, selon les cas, des outils informatiques et de communication.

La présente charte informatique a pour objectif de déterminer les conditions d'utilisation du système d'information et des outils informatiques par l'Utilisateur et de préciser les droits et devoirs de ce dernier.

Elle a également pour objet de sensibiliser les Utilisateurs aux risques liés à cette utilisation au regard de la sécurité informatique, de la pérennité du système, du respect de la vie privée et à la confidentialité des données. L'imprudence, la négligence ou la malveillance d'un Utilisateur peut entraîner des conséquences graves pour Sign IT et est un motif d'engagement de la responsabilité pénale ou civile d'un Utilisateur.

A cet égard, les Utilisateurs respectent une obligation générale de prudence et de confidentialité, et s'engagent à effectuer une utilisation raisonnée, mesurée et conforme aux stipulations de la Charte, du système d'information et des outils informatiques mis à disposition par Sign IT.

## **CHAMP D'APPLICATION**

La présente charte informatique fait partie intégrante du règlement intérieur de Sign IT et est contraignante à l'égard de tout Utilisateur à compter de son acceptation.

L'acceptation de la Charte intervient soit lors de sa mise en place, soit postérieurement à sa mise en place pour les nouveaux Utilisateurs.

Les intervenants extérieurs doivent s'engager à faire respecter la Charte par leurs propres salariés et leurs éventuels sous-traitants. Les contrats signés entre Sign IT et tout tiers ayant accès au système d'information et/ou aux outils informatiques doivent comporter une clause rappelant cette obligation.

La Charte est diffusée dans l'intranet de Sign IT et est mise à disposition de l'ensemble des Utilisateurs par voie électronique.

La Charte est susceptible d'être modifiée par Sign IT en fonction :

- Des évolutions du système d'information et des outils informatiques, en référence à l'état de l'art dans le domaine informatique.
- Des évolutions légales relatives aux stipulations de la présente Charte.

Le cas échéant, elle sera à nouveau soumise à acceptation des Utilisateurs et mise à disposition dans les conditions fixées plus haut.

Les droits et obligations résultants de la Charte ont force contraignante à l'égard des Utilisateurs dans le cadre de leur fonction, qu'elle soit exercée au sein même de Sign IT ou dans un tout autre lieu par la voie du télétravail.

## **PROTECTION DES DONNÉES PERSONNELLES**

Dans l'objectif de garantir le respect des obligations et des procédures prévus dans la Charte Informatique et pour permettre la gestion des outils informatiques, Sign IT est amené à collecter et à traiter des données à caractère personnel de l'Utilisateur (noms, prénom, qualité, identifiants, photographie, notamment).

En tant que responsable du traitement, Sign IT s'engage à effectuer tout traitement en conformité avec la réglementation relative aux données personnelles et en particulier au Règlement Général sur la Protection des Données (RGPD) entré en vigueur le 25 mai 2018. Les traitements réalisés au titre de la Charte sont fondés sur l'exécution d'un contrat matérialisé par la présente Charte à compter de son acceptation par l'Utilisateur.

Sign IT conserve les données personnelles correspondantes uniquement pendant la période de la relation contractuelle entre elle et l'Utilisateur. Au-delà, Sign IT s'engage à archiver les Données personnelles dans un but de constitution de preuve et à les supprimer à l'issue des délais de prescription légaux afférents.

Les seuls destinataires des Données personnelles sont les personnes internes à Sign IT et habilitées par elle à réaliser les traitements pour les finalités décrites ci-dessus.

L'Utilisateur peut exercer auprès de Sign IT, à tout moment, son droit d'accès, de rectification, et, dans les cas prévus par le Règlement 2016/679, son droit à la limitation, son droit d'opposition, son droit à l'effacement et son droit à la portabilité.

L'Utilisateur peut, s'il considère que ses droits au titre de la réglementation des données personnelles ne sont pas respectés et après avoir préalablement formulé sa demande et/ou ses observations auprès de Sign IT, contacter la CNIL.

# **PARTIE 1 : UTILISATION DU SYSTEME D'INFORMATION**

## **ARTICLE 1. ACCES AU SYSTEME D'INFORMATION**

### **1.1 – Accès**

L'accès au système d'information est sécurisé par un identifiant et un mot de passe, remis par le Service informatique. Celui-ci doit être changé lors de sa première connexion.

Cette identification permet, à chaque connexion, l'attribution de droits et privilèges propres à chaque utilisateur sur le système d'information dont il a besoin pour son activité.

Ce dernier est personnellement responsable de l'utilisation qui peut être faite de l'identifiant et du mot de passe.

### **1.2 - Politique des mots de passe**

La présente politique des mots de passe s'applique à tout compte qu'un utilisateur pourrait être amené à utiliser dans le cadre de son activité professionnelle.

Il est demandé à chaque utilisateur d'utiliser le gestionnaire de mots de passe de l'entreprise.

Un document expliquant comment créer un compte sur le gestionnaire de mots de passe est disponible, et les membres du support informatique trouveront un moment afin de former les utilisateurs si ces derniers se manifestent.

Il est interdit d'écrire des mots de passe ou phrases de passe, sur un document, livre ou autre support physique ainsi que sur un support virtuel non chiffré (exemple : bloc-notes, document Word, tableau Excel, etc...).

Il est formellement interdit de communiquer à un tiers n'importe quel mot de passe de l'entreprise ou de l'utilisateur, à l'exception des mots de passe permettant d'utiliser les produits de Sign IT, si l'autorisation a explicitement été donnée, ou est implicite, par exemple lors de la vente d'un produit à un client.

Les phrases de passe doivent comporter au moins 4 mots, 2 caractères spéciaux et une majuscule, pour un total d'au moins 20 caractères.

Un mot de passe doit comporter au moins 10 caractères et contenir des caractères provenant des quatre catégories suivantes :

- Caractère majuscule sans accent (A à Z)
- Caractère minuscule sans accent (a à z)
- Chiffres de 0 à 9, sans reprendre de numéro de téléphone.
- Caractère non alphabétiques (par exemple : !, %, #, \$, etc.)

Le mot de passe ou la phrase de passe ne doit pas contenir le login de l'utilisateur ou des parties de son nom complet, de celui de membres de sa famille, ou autres informations sur lui ou l'entreprise.

L'utilisation de l'authentification multi facteurs (MFA) est fortement recommandée sur les plateformes la supportant, bien que non obligatoire à cause des contraintes qu'elle pourrait représenter dans certains cas.

## ARTICLE 2. REGLES DE SECURITE DU SI

Tout utilisateur s'engage à respecter les règles de sécurité suivantes :

- Signaler au Service informatique toute violation ou tentative de violation suspectée de son compte utilisateur et de manière générale tout dysfonctionnement ;
- Signaler tout manquement à l'anonymisation de quelque donnée patient manipulée par Sign IT lors d'événements, de diffusion en direct, ou sur son système d'information ;
- Respecter le paragraphe 1.2, sur l'utilisation des mots de passe ;
- Ne jamais confier son identifiant/mot de passe à qui que ce soit ;
- Ne jamais demander son identifiant/mot de passe à un autre Utilisateur ;
- Utiliser le gestionnaire de mots de passe de l'entreprise.
- Ne jamais connecter au système d'information de périphérique provenant de l'extérieur de l'entreprise. Ceci englobe tout support amovible USB, matériel réseau, téléphone portable, etc... ;
- Ne pas usurper l'identité d'autrui, notamment dans ses communications électroniques ;
- Ne pas copier, modifier, détruire les logiciels sur lesquels Sign IT détient des droits de n'importe quelle nature ;
- Ne pas utiliser le système d'information de Sign IT pour y stocker des fichiers à des fins contraires à la loi, à l'ordre public ou à l'intérêt de Sign IT ;
- Ne pas utiliser le système d'information de Sign IT à des fins autres que professionnelles et dans le cadre des missions confiées par Sign IT ;
- Ne pas accéder ou tenter d'accéder à des fichiers, des informations, des systèmes ou des comptes pour lesquels l'Utilisateur n'a pas d'autorisation d'accès, ou de modification ;
- Toute copie de données sur un support externe est soumise à l'accord du supérieur hiérarchique et doit respecter les règles définies par Sign IT ;
- Vérifier l'identité des interlocuteurs à qui il s'adresse ;
- Faire très attention aux informations qu'il divulgue à l'oral et à l'écrit, ainsi qu'à toute forme d'ingénierie sociale auquel il pourrait être sujet.
- Ne communiquer d'informations, sur le système d'information, sur les produits, ou sur les membres de l'équipe, qu'aux personnes ayant besoin d'en connaître.
- Utiliser le tunnel VPN mis à disposition dès lors que l'utilisateur n'est pas sur le système d'information de Sign IT.
- Dès lors qu'il le peut, l'utilisateur doit chiffrer les données présentes sur son ordinateur professionnel et n'utiliser que des moyens de communication chiffrés pour, répondre à une demande d'authentification, s'authentifier sur un moyen informatique ou toute autre validation d'identité nécessaire pour son travail.
- Dans l'éventualité où l'Utilisateur serait amené à manipuler ou transporter, des données clients sur un support de stockage externe (enregistrements anonymisés de cas patient, enregistrements vidéo, photos etc...), celui-ci devra être chiffré selon les moyens mis à sa disposition par le SI.
- Tout équipement de communication collaborative est sujet aux mêmes règles de sécurité que l'ensemble des moyens de communications traditionnels. Les risques quant à leur usage sont souvent négligés et donc, ceux-ci ne doivent jamais être connectés ailleurs que sur le système d'information de Sign IT.
- Ne pas connecter aux logiciels de messagerie son/ses comptes de courriel personnel. Ne pas suivre les liens ni d'ouvrir et de télécharger de pièce jointe sur son compte courriel personnel. Si, ponctuellement, l'Utilisateur consulte son compte courriel

personnel, il doit utiliser la navigation privée de son navigateur.

Pour rappel, les règles et obligations de sécurité s'appliquent en tout temps et en tous lieux.

L'Utilisateur s'interdit de donner accès au système d'information à un tiers sans l'accord préalable de Sign IT.

L'Utilisateur est personnellement responsable de toute divulgation d'informations qui pourrait porter atteinte aux intérêts de Sign IT ou de ses clients. De la sorte, il s'engage à être particulièrement vigilant et prudent à chaque divulgation, quel que soit le destinataire, le mode de communication et son motif. L'obligation de vigilance pesant sur l'Utilisateur est renforcée en cas de divulgation par Internet et au moyen d'outils informatiques.



### **ARTICLE 3. RAPPEL DES PRINCIPES APPLICABLE EN CAS DE TRAITEMENT PORTANT SUR DES DONNEES PERSONNELLES**

Tout Utilisateur amené à traiter des Données personnelles dans le cadre de sa mission confiée par Sign IT doit respecter le Règlement n°2016/679 relatif à la protection des données à caractère personnel (ci-après le « Règlement »), et notamment les principes suivants :

- Respecter la finalité du traitement, ne pas utiliser les données auxquelles il peut accéder à des fins autres que celles prévues dans le cadre de sa mission ;
- S'assurer de la licéité du traitement ;
- Limiter la collecte de Données personnelles à celles strictement nécessaire à l'accomplissement de sa mission ;
- Ne conserver les données que pendant les durées définies préalablement par Sign IT pour chaque traitement, et à l'issue de cette période soit (i) effacer la donnée, (ii) anonymiser la donnée ou (iii) archiver la donnée sous certaines conditions.
- Ne faire aucune copie des données personnelles, sauf exception liée à l'exécution de la mission, et restituer la totalité des données en cas de cessation de la mission.
- Ne divulguer les données personnelles qu'aux personnes dûment autorisées en raison de leur mission.
- S'interdire de traiter une quelconque donnée personnelle sensible au sens de l'article 9 paragraphe 1 du Règlement précité, notamment des données de santé, sous réserve de rentrer dans l'un des cas prévus à l'article 9 paragraphe 2 du Règlement ;
- Assurer la sécurité des données personnelles dans le cadre des traitements et effectuer ces derniers avec la plus grande prudence, conformément aux obligations fixées par la présente Charte et aux politiques de confidentialité édictées par Sign IT ;
- S'assurer de l'information des personnes concernées par les traitements de données personnelles réalisés par Sign IT et collaborer, sur demande de Sign IT, à l'établissement de la documentation nécessaire à la conformité au Règlement ;
- Collaborer, le cas échéant et sur demande de Sign IT, en cas de demande d'exercice des droits par une personne concernée.

Pour rappel, tout manquement de Sign IT aux obligations fixées par le Règlement est passible d'une sanction administrative telle qu'une amende pouvant aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial.

Sign IT se réserve le droit d'agir contre l'Utilisateur responsable du manquement en question, et ce dans les conditions fixées à l'article 14 RESPONSABILITE – SANCTIONS.

## ARTICLE 4. INTERNET

Les Utilisateurs sont libres d'utiliser Internet, au sens large, sous réserve d'une utilisation présentant un lien direct et nécessaire avec l'activité professionnelle.

Toutefois, une utilisation d'Internet pour un motif personnel est admise sous réserve d'être ponctuelle, raisonnable, respectueuse des lois et de l'ordre public et qu'elle ne mette pas en cause ni les intérêts ni la réputation de Sign IT.

Il est strictement interdit d'utiliser le système d'information, le réseau Internet mis à disposition par Sign IT et les outils informatiques personnels ou mis à disposition par Sign IT pour, notamment :

- Emettre ou relayer des publications à caractère injurieux, raciste, diffamatoire ;
- Visiter des sites pornographiques ;
- Emettre ou relayer des actes de type harcèlement sexuel/moral.
- Effectuer des actes de concurrence déloyale vis-à-vis de Sign IT.
- Commettre des actions de malveillance, fraude, ou autre comportement illégal ;

Les données concernant l'utilisateur (sites consultés, messages échangés, etc...) peuvent être enregistrées par des tiers, analysées et utilisées à des fins notamment commerciales. Il est donc recommandé à chaque utilisateur de ne pas fournir son adresse électronique professionnelle, ni aucune coordonnée professionnelle sur internet, sauf si cette fourniture est strictement nécessaire à la conduite de son activité professionnelle.

Afin d'éviter les fuites d'informations, les tiers à la société Sign IT disposent de l'accès WIFI Invité uniquement et ne sont aucunement autorisés à utiliser les autres accès Wi-Fi, ni les câbles de connexion au réseau filaire.

De ce fait, et pour éviter tout manquement à cette règle, il est interdit à l'Utilisateur de communiquer la clé de sécurité du réseau Wi-Fi de Sign IT, que ce soit à un tiers ou une personne interne à Sign IT.

La clé de sécurité Wi-Fi du réseau de Sign IT est disponible sur la page d'accueil de l'intranet. Il est aussi possible de se présenter au Service Informatique afin de l'obtenir.

L'Utilisateur est autorisé à communiquer la clé de sécurité du réseau Wi-Fi INVITE à un tiers.

## **ARTICLE 5 – COMMUNICATION SUR INTERNET / RESEAUX SOCIAUX**

L'Utilisateur s'engage à respecter une obligation de réserve et de loyauté à l'égard de Sign IT dans le cadre de toute communication par ce dernier, qu'elle qu'en soit la forme ou la nature, d'informations relatives à Sign IT sur tous réseaux sociaux (Facebook, Twitter, Instagram, LinkedIn, etc.), blogs, forums de discussion, tribunes libres, sites de partage de photographies et/ou de vidéos dès lors que l'accès à ces informations communiquées par l'Utilisateur est libre.

A ce titre, l'Utilisateur s'engage à ne pas contrevenir aux dispositions de la loi du 29 juillet 1881 sur la liberté de la presse et s'abstenir de tout acte de dénigrement à l'encontre de Sign IT.

Pour participer à des forums, l'Utilisateur doit disposer d'autorisation internes afin de s'exprimer au nom de Sign IT.

## ARTICLE 6- MESSAGERIE PROFESSIONNELLE

### 6.1 - Accès à la messagerie

Une adresse électronique et un mot de passe est remis aux Utilisateurs internes à Sign IT. L'Utilisateur a la faculté de modifier le mot de passe qui lui a été confié et ce conformément à la politique de mots de passe (1.2.).

### 6.2 - Conditions d'utilisation

Afin d'éviter la surcharge informationnelle, il est recommandé à tous les utilisateurs de :

- S'interroger sur la pertinence de l'utilisation de la messagerie électronique professionnelle par rapport aux autres outils de communication disponibles ;
- S'interroger sur la pertinence des destinataires du courriel ;
- Utiliser avec modération les fonctions « CC » ou « Cci »
- S'interroger sur la pertinence des fichiers à joindre aux courriels ;
- Eviter l'envoi de fichiers trop volumineux et privilégier les liens sur serveur si envoi en interne ;
- Indiquer un objet précis permettant au destinataire d'identifier immédiatement le contenu du courriel ;

Afin d'éviter le stress lié à l'utilisation des outils informatiques et du système d'information, il est recommandé à tous les Utilisateurs de :

- S'interroger sur le moment opportun pour envoyer un courriel/SMS ou appeler un autre Utilisateur sur son téléphone professionnel (pendant les horaires de travail), il est possible de différer et planifier l'envoi d'un email ;
- Ne pas solliciter de réponse immédiate si ce n'est pas nécessaire ;
- Définir le « gestionnaire d'absence au bureau » sur la messagerie électronique et indiquer les coordonnées d'une personne à joindre en cas d'urgence ;
- Privilégier les envois différés lors de la rédaction d'un courriel en dehors des horaires de travail ;

Le transfert de messages, ainsi que leurs pièces jointes, à caractère professionnel sur des messageries personnelles est soumis aux mêmes règles que les copies de données sur support externes.

Les Utilisateurs peuvent consulter leur messagerie professionnelle à distance, à l'aide d'un navigateur (Webmail). Les fichiers qui seraient copiés sur l'ordinateur utilisé par l'Utilisateur dans ce cadre doivent être effacés dès que possible de l'ordinateur utilisé.

### 6.3 - Absence de l'Utilisateur et consultation de la messagerie

En cas d'absence physique d'un Utilisateur et afin de ne pas interrompre le fonctionnement du service, et après accord de la Direction, le Service informatique de Sign IT peut transmettre au Supérieur hiérarchique un message électronique à caractère exclusivement professionnel et identifié comme tel par son objet et/ou son expéditeur.

La personne désignée n'a pas accès aux autres messages de l'Utilisateur. L'Utilisateur concerné est informé dès que possible de la liste des messages qui ont été transférés.

En cas d'absence prolongée d'un Utilisateur, la personne désignée peut demander au Service informatique, après accord de la Direction le transfert des messages reçus.

### 6.4 - Courriel non sollicité

Sign IT dispose d'un outil permettant de lutter contre la propagation des messages non désirés (spam).

Aussi, afin de ne pas accentuer davantage l'encombrement du réseau lié à ce phénomène, les Utilisateurs sont invités à limiter leur consentement explicite préalable à recevoir un message de type commercial, newsletter, abonnements ou autres, et de ne s'abonner qu'à un nombre limité de listes de diffusion notamment si elles ne relèvent pas du cadre strictement professionnel.

## **ARTICLE 7. SERVICE INFORMATIQUE ET CONTRÔLE DES ACTIVITES.**

Le Service informatique assure le bon fonctionnement et la sécurité des réseaux, des moyens informatiques et de communication de Sign IT.

Le Service informatique dispose d'outils techniques afin de procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place. Il a accès à l'ensemble des données techniques mis, s'engageant à respecter les règles de confidentialité applicables aux contenus des documents. Il est assujéti au devoir de réserve et préserve la confidentialité des données qu'il est amené à connaître.

Pour des nécessités de maintenance et de gestion, l'utilisation des ressources matérielles ou logicielles, les échanges via le réseau, ainsi que les rapports des télécommunications peuvent être analysés et contrôlés dans le respect de la législation applicable, et notamment relatives à la protection de la vie privée et au respect des communications privées.

L'utilisateur est informé que pour effectuer la maintenance corrective, curative ou évolutive, le personnel du service informatique dispose de la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition, et qu'une maintenance à distance est précédée d'une information à l'utilisateur.

Réseau intranet : Sign IT peut vérifier à posteriori l'identité de l'utilisateur ayant accédé ou tenté d'accéder à une application au moyen du compte utilisé pour cet accès ou cette tentative d'accès.

Internet : Sign IT dispose des moyens techniques suivants pour procéder à des contrôles de l'utilisation de ses services :

- Limites d'accès au serveur proxy ;
- Pare-feu et anti-virus.

Sign IT garantit à l'utilisateur que seuls ces moyens de contrôle sont mis en œuvre.

Ces contrôles techniques sont effectués dans un souci de sécurité du système d'informations de Sign IT.

Sign IT se réserve, dans ce cadre, le droit de recueillir et de conserver les informations nécessaires à la bonne marche du système. Elle se réserve la possibilité de procéder à un contrôle des sites visités afin d'éviter l'accès par ces derniers à des sites illicites ou requérant l'âge de la majorité.

## **PARTIE 2- CONDITIONS D'UTILISATION DES OUTILS INFORMATIQUES**

### **ARTICLE 8- REMISE DES OUTILS ET ACCES**

#### **8.1 – Outils et moyens informatiques**

Sign IT met à disposition de l'Utilisateur les outils informatiques permettant de remplir les tâches inhérentes à son travail au sein de l'entreprise.

Les moyens informatiques mis à disposition sont, mais ne sont pas limités à :

- L'ordinateur professionnel ainsi qu'accessoires associés permettant son bon fonctionnement (écran, clavier et souris, hub USB, câbles...) ;
- Logiciels métiers divers ainsi que les accessoires éventuels permettant leur utilisation ou leur bon fonctionnement ;
- Logiciels et suites de logiciels permettant à l'Utilisateur d'accomplir et d'être performant dans ses tâches ;
- Matériel répondant à des besoins émanant des clients, de projets, ou en vue d'une installation
- Imprimantes et scanners ;
- Infrastructure logicielle et matérielle permettant aux utilisateurs de conserver et partager leurs données dans le respect des règlements en vigueur dans cette-même charte ;
- Boîte au lettre électronique, avec filtre anti-spam ;
- Téléphone fixe ou mobile professionnel ;
- Connexions à internet et intranet ;
- Outils de sauvegarde, disques durs amovibles et autres périphériques découlant d'une utilisation avancée des moyens informatiques ;

#### **8.2 - Besoins auxquels le système d'information doit répondre**

Le système d'information de Sign IT doit en permanence répondre aux besoins énoncés dans cet article.

Il est de la charge de l'Administrateur du système d'information que celui-ci réponde à toute heure aux besoins de l'Utilisateur et de Sign IT.

- Il doit répondre aux besoins opérationnels, organisationnels, stratégiques, réglementaires et collaboratifs de Sign IT ;
- Le système d'information doit se conformer aux lois françaises, européennes et mondiales en vigueur ;
- Les données du système d'information doivent être sauvegardées ;
- Il doit répondre aux attentes de l'Utilisateur, de la Direction, et des clients de Sign IT ;
- Il doit rester disponible 24h/24h et 7j/7 ;
- Être dimensionné et sécurisé proportionnellement ;

- Être documenté, afin de faciliter l'accès aux données, outils et autres moyens, et faciliter le transfert des compétences ;

#### **8.3 - Conditions de remise**

Ces outils, propriétés de Sign IT, sont remis à l'Utilisateur qui en assure la garde et un soin particulier au même titre que ceux que l'Utilisateur apporterait pour un outil personnel. Dans le cas où Sign IT met des outils informatiques à disposition de l'Utilisateur, ce dernier ne doit pas :

- Modifier ces équipements et leur fonctionnement, leur paramétrage, ainsi que leur configuration physique ou logicielle ;
- Utiliser un ordinateur ou téléphone autre que celui qui lui a été assigné pour accomplir

son travail ;

- Connecter ou déconnecter du réseau les outils informatiques sans y avoir été autorisé par le Service Informatique ;
- Déplacer l'équipement informatique (sauf s'il s'agit d'un « équipement nomade »)
- Nuire au fonctionnement des outils informatiques ;
- Utiliser les outils informatiques dans un but de dénigrement ou de concurrence déloyale à l'encontre de Sign IT.

Toute installation de logiciels supplémentaires est subordonnée à l'accord du Service informatique.

Chaque Utilisateur dispose d'un espace de stockage sur le serveur. Il est donc demandé à chaque Utilisateur de ne pas stocker de fichiers sur les disques durs internes aux Outils. En cas de perte ou de vol, les données seraient définitivement perdues.

#### 8.4 - Accès aux outils informatiques

L'accès aux ordinateurs portables, ordinateurs fixes, téléphones portables, smartphones, tablettes, et tout autre outil informatique comportant une fonction de verrouillage est sécurisé par un mot de passe conformément à la politique des mots de passe édictée au paragraphe 1.2.

L'Utilisateur est personnellement responsable de l'utilisation qui peut être faite du mot de passe.

## **ARTICLE 9. USAGE PROFESSIONNEL**

La messagerie et les outils informatiques mis à disposition des Utilisateurs par Sign IT sont destinés à un usage professionnel.

L'utilisation de la messagerie ou des outils informatiques à des fins personnelle est tolérée, à condition d'être raisonnable, ponctuelle et prudente, si elle n'affecte pas le travail de l'Utilisateur ni la sécurité du système d'information et des outils informatiques.

Il est demandé à l'Utilisateur de ne pas connecter son ou ses comptes de courriel personnels dans les logiciels de messagerie de son ordinateur, d'utiliser la navigation privée pour consulter ses courriels personnels, de ne pas ouvrir les pièces jointes ni de suivre un/des liens dans le cas d'une consultation de courriel personnel.

Tout doute de l'Utilisateur sur ces derniers points devra résulter en l'arrêt immédiat de l'usage personnel.

Tout document, message, mail, dossier, fichier qui comporte les mentions expresses « PERSONNEL » ou « PRIVE » bénéficie du droit au respect de la vie privée et du secret des correspondances. Sign IT s'engage à ne pas accéder aux fichiers comportant ces mentions.

A défaut de telles mentions, le document, message, mail, dossier, fichier est présumé professionnel.



## **ARTICLE 10. DROIT A LA DECONNEXION**

En vue d'assurer le respect des temps de repos et de congé ainsi que de la vie personnelle et familiale, chaque Utilisateur peut faire prévaloir son droit à la déconnexion professionnelle.

Sauf horaires décalés (travail de nuit ou le

week-end), ou cas d'extrême urgence pour des

raisons de sécurité, chaque Utilisateur disposant d'Outils pour des buts professionnels

s'engage à :

- Ne pas les utiliser les dimanches et jours fériés ;

- Ne pas les utiliser chaque jour de la semaine entre 20h00 et 07h00

- Ne pas contacter ou transmettre des données à un Utilisateur en congés ou en arrêt maladie.

Les responsables hiérarchiques s'abstiennent, dans la mesure du possible et sauf urgence avérée, de contacter leurs subordonnés en dehors de leurs horaires de travail telles que définies au contrat de travail ou par l'horaire collectif applicable au sein de Sign IT.

Dans tous les cas, l'usage de la messagerie électronique ou du téléphone professionnel en dehors des horaires de travail doit être justifié par la gravité, l'urgence et/ou l'importance du sujet en cause.

## **ARTICLE 11. OUTILS PERSONNELS**

L'évolution permanente des technologies de l'information confère aux Utilisateurs de nouveaux services disponibles depuis leurs propres matériels (à savoir notamment, ordinateurs portables, tablettes, smartphones, disques durs externes, clés USB, cartes mémoire, etc.). Ces matériels personnels sont susceptibles de présenter des risques de vulnérabilité, de saturation du réseau, et d'atteinte à la protection des données personnelles et/ou confidentielles, lorsqu'elles sont mises en œuvre par l'Utilisateur au sein de Sign IT, en particulier lorsqu'elles sont connectées aux Outils informatiques.

En cas d'impossibilité de faire autrement et dans le strict respect des dispositions de la Charte, seul les ordiphones (smartphones) pourront être connectés à Microsoft Teams, et ce uniquement via des ordiphones n'étant pas en fin de vie logicielle (ne recevant plus de mises à jour de sécurité), uniquement après explicite autorisation du service informatique. Cette mesure ne circonviend pas les mesures de sécurité mises en place et mentionnées dans la Charte.

En conséquence de ce qui précède, tout matériel personnel ne pourra être utilisé au sein de Sign IT qu'après autorisation du Service Informatique.

En tout état de cause, l'Utilisateur s'engage à ne pas procéder à la copie, reproduction et/ou enregistrement, sur tout support et matériel personnel, de quelque nature que ce soit, de toute information, qu'elle qu'en soit la forme ou la nature, afférente à Sign IT, qu'il en soit l'auteur ou l'utilisateur, sans l'autorisation écrite préalable expresse de Sign IT.

## **ARTICLE 12. PROPRIETE INTELLECTUELLE**

Il appartient à Sign IT d'acquérir les droits de propriété intellectuelle ou d'obtenir les autorisations nécessaires à l'utilisation du Système et des Outils mis à disposition des Utilisateurs.

Les Outils et le Système ne doivent en aucune manière être utilisées 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 de propriété intellectuelle, tels que des textes, images, photographies, œuvres musicales, œuvres audiovisuelles, logiciels et jeux vidéo, sans l'autorisation des titulaires des droits objets d'une protection au titre du code de la propriété intellectuelle et des conventions internationales applicables, lorsque cette autorisation est requise.

L'Utilisateur s'engage à se conformer à la politique de sécurité de Sign IT, y compris aux règles d'utilisation des moyens de sécurisation mis en œuvre dans le but de prévenir l'utilisation illicite des outils, et à s'abstenir de tout acte portant atteinte à l'efficacité de ces moyens.

Il est rappelé à cet égard que Sign IT, en sa qualité de titulaire d'un accès à Internet est tenue de sécuriser cet accès afin qu'il ne soit pas utilisé 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 de propriété intellectuelle.

Cette responsabilité du titulaire de l'accès n'exclut en rien celle de l'Utilisateur qui peut se voir reprocher un délit de contrefaçon (article L335-3 du code de la propriété intellectuelle)

## **ARTICLE 13. SUSPENSION / DEPART DE L'UTILISATEUR**

L'accès au système d'information est présumé avoir un caractère strictement professionnel, de sorte que la suspension du contrat de travail justifie sa suspension.

Lors de son départ, l'Utilisateur doit restituer au Service informatique les outils mis à sa disposition. Il doit préalablement effacer ses fichiers et données privées. Toute copie de documents professionnels doit être autorisée préalablement par la Direction.

Les comptes et les données personnelles de l'Utilisateur sont, en tout état de cause, supprimés dans un délai maximum d'un (1) an après son départ.

## ARTICLE 14. RESPONSABILITES – SANCTIONS

Le manquement aux règles et mesures de sécurité et de confidentialités définies par la Charte est susceptible d'engager la responsabilité de l'Utilisateur et d'entraîner des sanctions à son encontre. Des sanctions en interne peuvent être prononcées, elles consistent :

- Dans un premier temps, en un rappel à l'ordre émanant du Service informatique, après avis du directeur de Site, en cas de non-respect des règles énoncées par la Charte ;
- Dans un second temps, et en cas de renouvellement, après avis du Directeur de site et du Responsable hiérarchique de l'Utilisateur, en des sanctions disciplinaires adoptées après saisine du comité consultatif paritaire restreint.
- Enfin, le non-respect des lois et textes applicables en matière de sécurité des systèmes d'information est susceptibles de sanctions pénales ou civiles prévues par la loi.

Les sanctions disciplinaires adoptées par Sign IT relativement à la présente Charte ne sont pas exclusives, en fonction de la gravité du manquement, d'un engagement de la responsabilité civile ou pénale de l'Utilisateur.

La présente Charte entre en vigueur à compter du 1 Janvier 2024.

Signature de la direction :

A handwritten signature in black ink, appearing to be a stylized 'D' or 'P' with a large loop at the top and several horizontal strokes at the bottom.

Signature du concerné :

Killian VIENNE