**ANNEXE 13 : EXEMPLE DE CHARTE INFORMATIQUE**

*La présente charte informatique est un exemple qu’il convient d’adapter au fonctionnement particulier de chaque SSTI.*

*Son objet est de proposer une base de rédaction reprenant en compte les exigences du RGPD en matière d’obligations des utilisateurs concernant à la fois les bonnes pratiques en matière d’utilisation du système d’information et les équipements informatiques des SSTI par les utilisateurs (principalement les salariés) afin de protéger au maximum la confidentialité, l’intégrité et la sécurité des données personnelles.*

\* \* \*

**PREAMBULE**

Le SSTI met en œuvre un système d’information et de communication nécessaire à son activité, comprenant notamment un réseau informatique et téléphonique, ainsi que des équipements informatiques fixes et mobiles.

Les salariés, dans l’exercice de leurs fonctions, sont conduits à accéder et à utiliser lesdits équipements informatiques, ainsi que les systèmes d’information et de communication mis à leur disposition.

L’utilisation du système d’information et de communication doit être effectuée exclusivement à des fins professionnelles, sauf exception prévue dans la présente charte.

Par ailleurs, des tiers au SSTI (salariés suivis, prestataires externes, partenaires…) peuvent également avoir accès aux équipements informatiques et aux systèmes d’information et de communication du SSTI.

Or, l’utilisation d’équipements informatiques (hardware et software), de réseaux de communication et du système d’information fait peser un risque pour le SSTI concernant le fonctionnement, la sécurité et l’intégrité de son système d’information et de communication, mais également concernant les données (à caractère personnel ou non, sensibles ou non) qui sont traitées dans le cadre de l’activité du SSTI.

Aussi, dans un but de transparence à l’égard des utilisateurs, de promotion d’une utilisation loyale, responsable et sécurisée du système d’information et des équipements informatiques, la présente charte pose les règles relatives à l’utilisation de ces ressources et ce notamment dans le respect des règles spécifiques aux professionnels de santé.

Cette charte a pour objectifs :

* de sensibiliser les utilisateurs aux risques liés à la sécurité informatique en matière de libertés et de vie privée, notamment à travers les traitements de données à caractère personnel qu’ils sont amenés à effectuer ;
* d’informer les utilisateurs sur :
  + les usages permis des moyens informatiques mis à sa disposition ;
  + les règles de sécurité en vigueur ;
  + les mesures de contrôle prises par le SSTI ;
  + les sanctions éventuellement encourues par les utilisateurs ;
* de formaliser les règles générales de sécurité que les utilisateurs s’engagent à respecter, en contrepartie de la mise à disposition des systèmes d’information et des équipements informatiques, et ainsi de déterminer les droits et devoirs des utilisateurs.

Ces règles s’inscrivent dans une démarche responsable afin de protéger d’une part le patrimoine informationnel et l’image de marque de SSTI, et d’autre part les libertés et la vie privée des personnes concernées que sont les salariés du SSTI et les tiers en lien avec les SSTI (salariés suivis, prestataires externes, partenaires…).

Le Responsable des systèmes d’information et la Direction se tiennent à la disposition des utilisateurs qui souhaiteraient disposer d’informations ou de conseils complémentaires relatifs à l’usage des systèmes d’information et des équipements informatiques.

**DEFINITIONS**

**« Equipements informatiques »** : désigne l’ensemble des matériels, équipements, outils informatiques mis à disposition par le SSTI aux Utilisateurs.

**« Personnes concernées »** : désigne les personnes physiques dont les données à caractère personnel sont traitées par le SSTI ou par tout tiers via le système d’information ou de communication du SSTI, ou via des Equipements informatiques.

**« Utilisateurs »** : désigne toute personne qui utilise les systèmes d’information du SSTI et les Equipements informatiques quel que soit son statut, et notamment les mandataires sociaux, les salariés, les intérimaires, les stagiaires, les employés de sociétés prestataires, les visiteurs occasionnels, les salariés suivis et de manière générale, à toute personne qui a obtenu un droit d’utilisation du système d’information du SSTI ou de ses Equipements informatiques.

**CHAMP D’APPLICATION**

1. **Utilisateurs concernés**

Sauf mentions contraires, la présente charte s’applique à tous les Utilisateurs tels que définis ci-avant.

La présente charte devra être annexée au contrat de prestations conclus avec des tiers, qui s’engageront à la respecter.

Par ailleurs, tout utilisateur extérieur au SSTI ne peut avoir accès au système d’information du SSTI qu’en présence d’une autorisation expresse et écrite préalable délivrée par le responsable du SI, et doit s’engager à respecter l’ensemble des dispositions de la présente charte.

A ce titre, et d’une manière générale, les salariés doivent veiller à faire accepter valablement la présente charte à toute personne à laquelle ils permettraient l’accès au SI.

1. **Système d’information et de communication**

La présente charte concerne l’ensemble des moyens informatiques et de communication électronique qui sont mis à la disposition des utilisateurs à des fins professionnelles, ainsi que l’ensemble des moyens informatiques et de communication électronique qui sont la propriété personnelle de l’utilisateur, et pour lesquels celui-ci a obtenu une autorisation d’utilisation dans le cadre de son activité professionnelle.

Les systèmes d’information et de communication su SSTI sont notamment constitués des éléments suivants :

* ordinateurs portables ou fixes
* périphériques (y compris clés USB)
* réseaux informatiques (serveurs, routeurs, connecteurs)
* photocopieurs
* télécopieurs
* téléphones (fixes et portables) et smartphones
* tablettes électroniques
* logiciels
* fichiers informatiques et bases de données
* espaces de stockage individuel
* messagerie
* connexions internet, intranet, extranet.

1. **Dérogations possibles**

Toute demande de dérogation aux différents éléments définis dans le cadre de la présente Charte doit être présentée par écrit à la direction des systèmes d’information, et en particulier au responsable des systèmes d’information. La décision finale est ensuite prise en concertation avec la direction générale qui se réserve le droit d’accepter ou de refuser les demandes de dérogation.

1. **Instances représentatives du personnel**

Toute utilisation des outils technologiques mis en place par le SSTI pour ses utilisateurs est strictement et expressément interdite à des fins syndicales et/ou de revendications pour quelque cause que ce soit.

Les membres des IRP sont soumis aux autres dispositions de la présente charte.

Dans le cadre de leur mandat, les correspondances et informations échangées et stockées par les IRP sont, par principe, confidentielles et ne sont pas susceptibles d’être contrôlées, sauf lorsqu’un texte le prévoit.

La présente charte a été soumise pour avis aux IRP.

**ACCES AUX SYSTEMES D’INFORMATION ET AUX OUTILS DE COMMUNICATION**

L'accès à certains éléments du système d'information (comme la messagerie électronique ou téléphonique, les sessions sur les postes de travail, le réseau, certaines applications ou services interactifs) est protégé par des paramètres de connexion (identifiant, mot de passe).

Ces paramètres sont personnels à l'utilisateur et doivent être gardés confidentiels. Ils permettent en particulier de contrôler l'activité des utilisateurs. Il ne doivent être communiqués à personne, ni responsable hiérarchique, ni informatique. Dans la mesure du possible, ces paramètres doivent être mémorisés par l'utilisateur et ne pas être conservés, sous quelque forme que ce soit. En tout état de cause, ils ne doivent pas être transmis à des tiers ou aisément accessibles. Ils doivent être saisis par l'utilisateur à chaque accès et ne pas être conservés en mémoire dans le système d'information.

Lorsqu'ils sont choisis par l'utilisateur, les paramètres doivent respecter un certain degré de complexité et être modifiés régulièrement. Des consignes de sécurité sont élaborées par la direction ou la direction informatique afin de recommander les bonnes pratiques en la matière.

L’utilisateur s’engage à respecter les considérations d’efficacité du mot de passe qui lui sont ainsi transmises, lesquelles dépendent du nombre de caractères alphanumériques (X caractères au moins, et autres spécificités….), de son originalité, de son renouvellement régulier par l’utilisateur (tous les Y mois,…).

Aucun utilisateur ne doit se servir pour accéder au système d’information de l’entreprise d’un autre compte que celui qui lui a été attribué. Il ne doit pas non plus déléguer à un tiers les droits d’utilisation qui lui sont attribués.

Ce droit d’accès cesse automatiquement lors d’un départ (l’utilisateur quittant le SSTI, fin de contrat) et peut être modifié lors d’un changement d’affectation (changement de poste, mutation, etc.) ou s’il est constaté que l’utilisateur a enfreint l’une des obligations imposées par la présente charte.

**MESSAGERIE ELECTRONIQUE**

1. **Principes généraux**

Chaque salarié dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique normalisée attribuée par la direction informatique.

Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam.

Les salariés sont invités à informer la direction informatique des dysfonctionnements qu'ils constateraient dans ce dispositif de filtrage.

L’attention des utilisateurs est attirée sur le fait qu’un message électronique a la même portée qu’un courrier manuscrit et peut rapidement être communiqué à des tiers. Il convient de prendre garde au respect d’un certain nombre de principes, afin d’éviter les dysfonctionnements du système d’information, de limiter l’envoi de messages non sollicités et de ne pas engager la responsabilité civile ou pénale du SSTI et/ou de l’utilisateur.

Les utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances 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.

Les risques liés à l’interception des messages électroniques des utilisateurs exigent de limiter l’utilisation de la messagerie électronique à destination de l’extérieur du système d’information aux informations à caractère non confidentiel et/ ou non sensible. L’utilisateur doit consulter le responsable des systèmes d’information en cas du moindre doute, sauf dérogation expresse donnée par le responsable des systèmes d’information.

La vigilance des utilisateurs doit redoubler en présence d’informations à caractère confidentiel. Les messages doivent dans ce cas être cryptés, conformément aux recommandations du responsable des systèmes d’information.

Pour des raisons de capacité mémoire, les messages électroniques sont conservés sur le serveur de messagerie pendant une durée maximale de \_\_ an(s). Passé ce délai, ils sont automatiquement supprimés. Si l’utilisateur souhaite conserver des messages au-delà de ce délai, il lui appartient d'en faire des sauvegardes avec l’aide de la direction informatique si nécessaire. Il est aussi tenu de supprimer lui-même dès que possible tous les messages inutiles.

1. **Concernant l’envoi de messages électroniques**

Avant tout envoi, il est impératif de bien vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises. En présence d’informations à caractère confidentiel, de données à caractère personnel ou de données sensibles, ces vérifications doivent être renforcées ; en cas de besoin, un cryptage des messages pourra être aussi proposé par la direction informatique.

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, de contrôler la liste des abonnés et de prévoir l’accessibilité aux archives.

Le risque de retard, de non remise et de suppression automatique des messages électroniques doit être pris en considération pour l'envoi de correspondances importantes.

Les messages importants doivent être envoyés avec un accusé de réception ou signés électroniquement.

Ils doivent, le cas échéant, être doublés par un envoi de fax ou de courrier postal.

La forme des messages professionnels doit respecter les règles définies par la direction, pour ce qui concerne la mise en forme et surtout la signature des messages.

La signature des courriers électroniques fait l’objet d’une forme standardisée [cf. charte graphique si elle existe]. Chaque utilisateur s’engage à respecter cette forme en évitant tout élément complémentaire.

1. **Concernant la réception de messages électroniques**

L’utilisateur ne doit pas ouvrir, ni répondre à des messages électroniques suspects tels que spam, messages électroniques répétés, messages sans texte avec pièce jointe non-identifiée, message sans lien avec l’activité du SSTI ou de l’utilisateur, message non-identifié, ni les transférer lorsque ceux-ci sont reçus à son insu sur leur messagerie électronique professionnelle et ne présentent aucun rapport avec ses fonctions et ses attributions au sein de SSTI.

Il s’engage, dans pareil cas, à les détruire immédiatement et à avertir le responsable des systèmes d’information en cas d’abus manifeste de fréquence ou de volume.

1. **Concernant l’absence des utilisateurs**

En cas d’absence supérieure à trois jours, l’utilisateur devra activer la fonction de délégation ou de notification d’absence afin de prévenir toute discontinuité dans le traitement des messages et permettre à ses interlocuteurs de prendre des mesures appropriées.

L’utilisateur est informé et accepte qu’en cas d’absence prolongée ou pour la continuité des services, la direction des systèmes d’information se réserve le droit d’accéder à sa messagerie et à ses dossiers professionnels, et ce sans son consentement préalable.

A ce titre, et afin d'éviter l'interception de tout message destiné à une institution représentative du personnel, les messages présentant une telle nature doivent être signalés et classés de la même manière que les messages à caractère personnel, mais en utilisant la mention "Délégué" dans leur objet à l’émission et dans le dossier où ils doivent être classés.

1. **Utilisation personnelle de la messagerie**

Les messages à caractère personnel sont tolérés, à condition de respecter la législation en vigueur, de ne pas perturber et de respecter les principes posés dans la présente charte.

Les messages envoyés doivent être signalés par la mention "Privé" ou "Perso" dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé de la même façon.

Les messages reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé "Privé" ou "Perso".

En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.

Toutefois, les utilisateurs sont invités, dans la mesure du possible, à utiliser leur messagerie personnelle pour l'envoi de messages à caractère personnel plutôt que la messagerie de l’entreprise.

**TELEPHONIE**

1. **Principes généraux**

Pour leur activité professionnelle, les utilisateurs peuvent disposer d’un téléphone fixe et/ou mobile, d’un smartphone, d’une tablette ou d’’une clé 3G.

Concernant l’utilisation des terminaux mobiles en connexion pour accès à des sites Internet ou à la messagerie électronique, les règles édictées dans la présente charte s’appliquent identiquement.

De plus, il est 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.

L’utilisateur est informé qu’un journal des communications, entrantes et/ou sortantes, est accessible par le SSTI s’agissant tant de la téléphonie fixe que mobile. Les utilisateurs sont informés que les relevés de communication peuvent faire l’objet d’un contrôle.

Les applications mises en place sur les smartphones peuvent permettre aux utilisateurs de se géolocaliser. Cependant, les utilisateurs ne doivent pas mettre en œuvre ces processus de géolocalisation et sont informés qu’en cas de géolocalisation, le SSTI pourra avoir accès à cette information.

1. **Engagements de l’utilisateur**

L’utilisateur s’engage à :

* prévenir sans délai en cas de perte, vol ou faille de sécurité ;
* mettre en œuvre tous les moyens de sécurité prévus par les fonctionnalités du smartphone et qui sont demandées et notamment le code d’accès ;
* utiliser des codes d’accès (pin, verrouillage clavier et autre) différents ;
* se déconnecter de toutes applications après usage et ne pas rester connectés par défaut ;
* être vigilants vis à vis des données contenues dans le smartphone.

1. **Utilisation personnelle de la téléphonie**

L’utilisation à caractère personnel du téléphone, fixe ou mobile, est tolérée, à condition qu’elle reste dans des limites raisonnables en termes tant de temps passé que de quantité d’appels.

Les surcoûts pour l’entreprise engendrés par l’utilisation de la téléphonie à des fins personnelles devront être remboursés par les utilisateurs concernés. Il s’agit tout particulièrement des appels à des numéros surtaxés et des appels depuis l’étranger ou à destination de l’étranger, au sens de la facturation téléphonique.

Les utilisateurs sont informés que la direction informatique enregistre leur activité téléphonique, aussi bien sur les postes fixes que sur les mobiles. Ces traces seront exploitées à des fins de statistiques, contrôle et vérification dans les limites prévues par la loi.

Toutefois, seule la direction pourra avoir accès aux numéros détaillés, permettant d’identifier les interlocuteurs d’un utilisateur, et seulement en cas de différend avec lui.

**INTERNET / EXTRANET**

Dans le cadre de leur activité, les utilisateurs peuvent avoir accès à Internet.

Le responsable des systèmes d’informations, pour des raisons de sécurité, peut limiter ou prohiber l’accès à certains sites. Celui-ci est habilité à imposer des configurations du navigateur et à restreindre le téléchargement de certains fichiers.

La contribution des utilisateurs à des forums de discussion, systèmes de discussion instantanée, blogs, sites est interdite ou autorisée sous réserve d’autorisation préalable du responsable des systèmes d’information. Un tel mode d’expression est susceptible d’engager la responsabilité du SSTI, une vigilance renforcée des utilisateurs est donc indispensable.

Il est rappelé que les utilisateurs ne doivent en aucun cas se livrer à une activité illicite ou portant atteinte aux intérêts du SSTI, y compris sur Internet.

Pour des raisons de sécurité ou de déontologie, l'accès à certains sites peut être limité ou prohibé par la direction informatique qui est habilitée à imposer des configurations du navigateur et à installer des mécanismes de filtrage limitant l’accès à certains sites.

Seule la consultation de sites ayant un rapport avec l’activité professionnelle est autorisée.

En particulier, sont interdits :

* l’utilisation de l’Internet à des fins commerciales personnelles en vue de réaliser des gains financiers ou de soutenir des activités lucratives
* la création ou la mise à jour au moyen de l’infrastructure du SSTI tout site Internet, notamment des pages personnelles.
* la connexion 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 du système d’information du SSTI ou engageant financièrement celle-ci.

**ACCES AUX SYSTEMES D’INFORMATION ET DE COMMUNICATION EXTERNE (EN DEHORS DU SSTI : TELETRAVAIL, EN CLIENTELE, ACCES AU BUREAU A DISTANCE…)**

Le présent article concerne l’utilisation des systèmes d’information du SSTI, de ses ressources, et des moyens de communication par l’utilisateur lorsque celui-ci est situé en-dehors du site physique du SSTI.

En premier lieu, il convient de préciser que l’ensemble des dispositions de la présente charte sont applicables aux utilisateurs accédant aux systèmes d’information et de communication du SSTI à distance.

Par ailleurs, il est impératif que l’utilisateur informe préalablement le responsbale du système d’information des accès à distance qu’il mettra en place, afin d’en obtenir préalablement l’autorisation et que lui soient communiquées les consignes de sécurité et de confidentialité propres à sa situation.

Tout accès à distance par du matériel informatique personnel est interdit sauf autorisation expresse et écrite de la part du responsable du SI.

**DONNEES A CARACTERE PERSONNEL – DONNEES SENSIBLES**

La Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite Loi Informatique et Libertés, ainsi que le Règlement général sur la protection des données (RGPD) viennent définir les conditions dans lesquelles des traitements de données à caractère personnel peuvent être opérés.

La Loi Informatique et Libertés et le RGPD instituent au profit des Personnes Concernées par les traitements réalisés par les Utilisateurs des droits que la présente charte vient protéger et respecter, tant à l’égard des utilisateurs que des tiers.

A cet égard, les Utilisateurs s’engagent à :

* ne pas utiliser les données à caractère personnel auxquelles ils peuvent accéder à des fins autres que celles prévues par leurs attributions ;
* ne divulguer ces données qu’aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu’il s’agisse de personnes privées, publiques, physiques ou morales ;
* ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l’exécution de leurs fonctions ;
* prendre toutes les mesures conformes aux usages et à l’état de l’art dans le cadre de leurs attributions afin d’éviter l’utilisation détournée ou frauduleuse de ces données ;
* prendre toutes précautions conformes aux usages et à l’état de l’art pour préserver la sécurité physique et logique de ces données ;
* d’assurer, dans la limite de leurs attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
* ne pas accéder, tenter d’accéder ou supprimer les données en dehors de leurs attributions ;
* respecter les droits des personnes concernées (droit d’accès, de rectification, d’opposition, effacement…) conformément aux procédures mises en place par le SSTI ;
* en cas de cessation de leurs fonctions, restituer intégralement les données, fichiers informatiques et tout support d’information relatif à ces données.
* respecter l’ensemble des procédures liées à la protection des données mises en place par le SSTI, et à respecter et favoriser l’ensemble des mesures techniques et organisationnelles mises en place par le SSTI afin de se conformer à la réglementation applicable.

Il convient de rappeler qu’en vertu de la Loi Informatique et du Règlement, le SSTI et les Utilisateurs peuvent être passibles de sanctions importantes, qu’elles soient administratives, civiles ou pénales.

Aussi, les Utilisateurs s’engagent, par le respect de la présente charte, à respecter les principes fondamentaux de la protection des données à caractère personnel, à savoir notamment la minimisation de la collecte et la préservation de la confidentialité, de l’intégrité et de la sécurité des données à caractère personnel.

Les utilisateurs sont au cœur de la protection des données à caractère personnel, et par conséquent des libertés et de la vie privée des personnes concernées.

Il leur appartient donc de respecter à cet effet l’ensemble des obligations leur incombant en vertu de la présente charte et des textes législatifs qui pourraient leur être appliqués.

**Il convient enfin d’indiquer que compte tenu du caractère sensible de certaines données à caractère personnel traitées par le SSTI, les utilisateurs se doivent de faire preuve de la plus grande vigilance possible concernant la protection des données.**

**CONFIDENTIALITE**

Le respect de la confidentialité des données, à à caractère personnel ou non, est une exigence essentielle.

La sauvegarde des intérêts du SSTI nécessite le respect d'une obligation générale et permanente de confidentialité et de secret professionnel, à l'égard des données disponibles mises à la disposition de l'utilisateur pour l'exercice de son activité professionnelle dans le cadre notamment de l’utilisation des systèmes d’information.

En conséquence, l’utilisateur s’engage au respect de la présente charte et des textes en vigueur, notamment en veillant à ce que les tiers non autorisés n'aient pas connaissance de telles informations, conformément aux règles d'éthique professionnelle ou de déontologie, le cas échéant.

Il est interdit d'utiliser des moyens de cryptologie autres que ceux expressément autorisés par le SSTI.

La transmission de données (à caractère personnel ou non) ne peut être réalisée qu'aux conditions suivantes :

* habilitation de l'émetteur ;
* désignation d'un destinataire autorisé ;
* respect d'une procédure sécurisée.

Le SSTI se réserve, pour quelque raison que ce soit, de manière temporaire ou définitive, le droit d'accorder, de refuser, de modifier ou de supprimer tout ou partie, le droit d'accès de toute personne pour des raisons liées directement à la continuité et la sécurité des services.

**SECURITE**

1. **Principes généraux**

Du fait de la collecte de données et du traitement de celles-ci réalisés, le SSTI s'engage, dans le cadre des dispositions légales et réglementaires qui s’imposent à lui et dans le respect du principe de proportionnalité édicté par le RGPD, à mettre en œuvre toutes les mesures organisationnelles et techniques utiles afin de préserver la sécurité, l’intégrité et la confidentialité des Données, ainsi que la sécurité de son système d’information et de communication, sur le plan technologique et procédural, afin notamment d’empêcher toute modification, tout transfert et toute suppression non-autorisés des Données, et toute intrusion non-autorisée dans son système d’information ou son endommagement.

Toutefois, le premier risque reste le risque humain lié aux traitements et aux manipulations des Données par les Utilisateurs, et par l’utilisation par ces derniers du système d’information et de communication et des outils qui y sont liés.

Par conséquent, la mise en place d'outils de sécurité ne doit pas dispenser les utilisateurs de signaler toute tentative d'intrusion extérieure, de falsification ou de présence de virus au responsable des systèmes d'information.

Tout utilisateur a la charge, à son niveau, de contribuer à la sécurité des moyens mis à sa disposition et du réseau auquel il a accès, principalement en évitant l'intrusion de virus susceptibles d'endommager le système d'information de SSTI.

1. **Obligations de l’Utilisateur**

Dans ce cadre, et outre les obligations incombant aux Utilisateurs mentionnées ci-avant et ci-après, l’Utilisateur s’engage à :

* ne pas stocker ou router des gadgets reçus ou trouvés sur internet ;
* ne pas modifier la configuration de son poste de travail informatique telle qu’effectuée par la direction des systèmes d’information ;
* ne pas permettre à tout tiers non-autorisé un accès aux systèmes d’information et de communication, à travers tout matériel informatique ;
* ne pas utiliser des éléments d’identification (identifiant/mot de passe), ou ne pas tenter d’utiliser des éléments d’identification, autres ceux qui lui sont attribués par le SSTI ;
* informer sans délai sa hiérarchie et le responsable du système d’information de tout dysfonctionnement du système d’information et de communication, toute altération, perte, vol, destruction des Données ou autre évènement pouvant affecter le système d’information, de communication ou les Données ;
* ne pas installer, tenter d’installer, utiliser ou tenter d’utiliser des logiciels informatiques sans l’accord de sa hiérarchie et du responsable du système d’information ;
* supprimer ou tenter de supprimer les logiciels installés sur le matériel qu’il utilise ;
* na pas accéder au système d’information avec du matériel personnel ou de tiers, sauf accord du responsable du système d’information ;
* ne pas sortir les Equipements informatiques du SSTI en dehors du site du SSTI, sauf accord du responsable du système d’information ;
* effectuer des sauvegardes régulières des fichiers et Données dont il dispose, suivant les procédures mises en place par le SSTI ;
* respecter l’ensemble des droits des tiers, et notamment de propriété intellectuelle ;
* ne pas télécharger de fichiers, en particulier médias, sans rapport avec l’activité professionnelle ou présentant un risque pour le système d’information ;
* verrouiller son ordinateur à chaque fois qu’il quitte son poste de travail ;
* ne pas transmettre ses identifiants de connexion (identifiant/mot de passe)
* respecter les procédures mises en place par le SSTI ;
* utiliser les logiciels dans les conditions de licence souscrites.

A ce titre, l’Utilisateur est informé que la contrefaçon est un délit passible de sanctions civiles et pénales et que l’utilisation des systèmes d’information et de communication implique le respect des droits de propriété intellectuelle des éditeurs, de ses partenaires du SSTI et de tout tiers titulaire de droits.

L’Utilisateur est invité à contacter le responsable du système d’information en cas de doute sur l’utilisation des Equipements informatiques, du système d’information ou du système de communication.

**CONTROLE DES ACTIVITES**

Les Utilisateurs sont informés que le SSTI met en place des outils afin de surveiller l’activité du système d’information et de communication.

Sont notamment surveillées et conservées les données relatives :

* à l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications et suppressions de fichiers ;
* aux connexions entrantes et sortantes au réseau interne, à la messagerie et à Internet, pour détecter les anomalies liées à l'utilisation de la messagerie et surveiller les tentatives d'intrusion et les activités, telles que la consultation de sites 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.

L'attention des utilisateurs est attirée sur le fait qu'il est ainsi possible de contrôler leur activité et leurs échanges. Des contrôles automatiques et généralisés sont susceptibles d’être effectués pour limiter les dysfonctionnements, dans le respect des règles en vigueur.

L’utilisateur est informé que le responsable des systèmes d’information, dont la fonction est de veiller au fonctionnement normal et à la sécurité des réseaux et systèmes informatiques, est conduit de par ses fonctions, à avoir accès à l’ensemble des informations relatives aux utilisateurs (messages, connexion à Internet, etc.), y compris à celles qui sont enregistrées sur le disque dur de leurs postes de travail.

Il demeure cependant soumis aux règles encadrant le secret professionnel et de confidentialité.

En cas de suspicion de manquement(s) grave(s) aux dispositions de la présente charte, la direction pourra procéder à toutes les mesures d’investigation utile, dans le respect des règles en vigueur.

Tout logiciel installé illicitement ou tout fichier suspect sera supprimé par le responsable des systèmes d’information dès le constat de leur présence sur le poste de travail.

Le caractère « non professionnel » des répertoires informatiques clairement identifiés comme « privé » ou « personnel », ne fait pas obstacle à des modalités de contrôle dans les conditions précitées.

**SANCTIONS**

Il est rappelé que la présente charte est document à portée juridique, et donc contraignante pour les Utilisateurs.

En effet, le manquement aux règles et mesures de sécurité décrites dans la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés.

Dans ce dernier cas, les procédures prévues dans le règlement intérieur et dans le Code du travail seront appliquées.

L’utilisation reconnue à des fins personnelles de certains services payants à travers le système de communication de l’entreprise donnera également lieu à remboursement de la part de l’utilisateur concerné.

Le SSTI se réserve également le droit d’engager ou de faire engager des poursuites pénales et/ou civiles, indépendamment des sanctions disciplinaires mises en œuvre, notamment mais pas limitativement en cas de fraude informatique, de non-respect des droits d’auteur ou de violation du secret des correspondances.

A ce titre, il est précisé que le responsable des systèmes d’information peut effacer, isoler et conserver aux fins de preuve toute trace de logiciels, progiciels, programmes ou fichiers créés ou introduits dans le système d’Information de SSTI, en violation des droits des tiers, notamment de propriété intellectuelle, et dénoncer tout acte délictueux aux autorités, sans préjudice de l’application de sanctions envers l’Utilisateur.

**INFORMATION**

La présente charte est affichée publiquement en annexe du règlement intérieur.

Elle est communiquée individuellement à chaque salarié par voie électronique.

La direction informatique est à la disposition des salariés pour leur fournir toute information concernant l'utilisation du système d’information, en particulier sur les procédures de sauvegarde, de sécurité et de droit des Personnes Concernées.

Elle les informe régulièrement sur l'évolution des limites techniques du système d'information et de communication ainsi que sur les menaces susceptibles de peser sur sa sécurité.

Chaque utilisateur doit se conformer aux procédures et règles de sécurité édictées par la direction informatique dans le cadre de la présente charte.

En cas de besoin, les salariés pourront être formés par la direction informatique pour appliquer les règles d'utilisation du système d’information et de communication prévues.