CHARTE ACCÈS ET USAGES DU SYSTÈME D'INFORMATION – UTILISATEUR

[Nom de l'ESMS / Organisme gestionnaire]

Note : Ce document est un exemple de charte à adapter et compléter par chaque ESMS. Les champs entre crochets [ ] doivent être remplacés par les informations spécifiques à votre établissement. Cette charte n'a pas de valeur juridique tant qu'elle n'est pas validée et signée par la direction de l'ESMS.

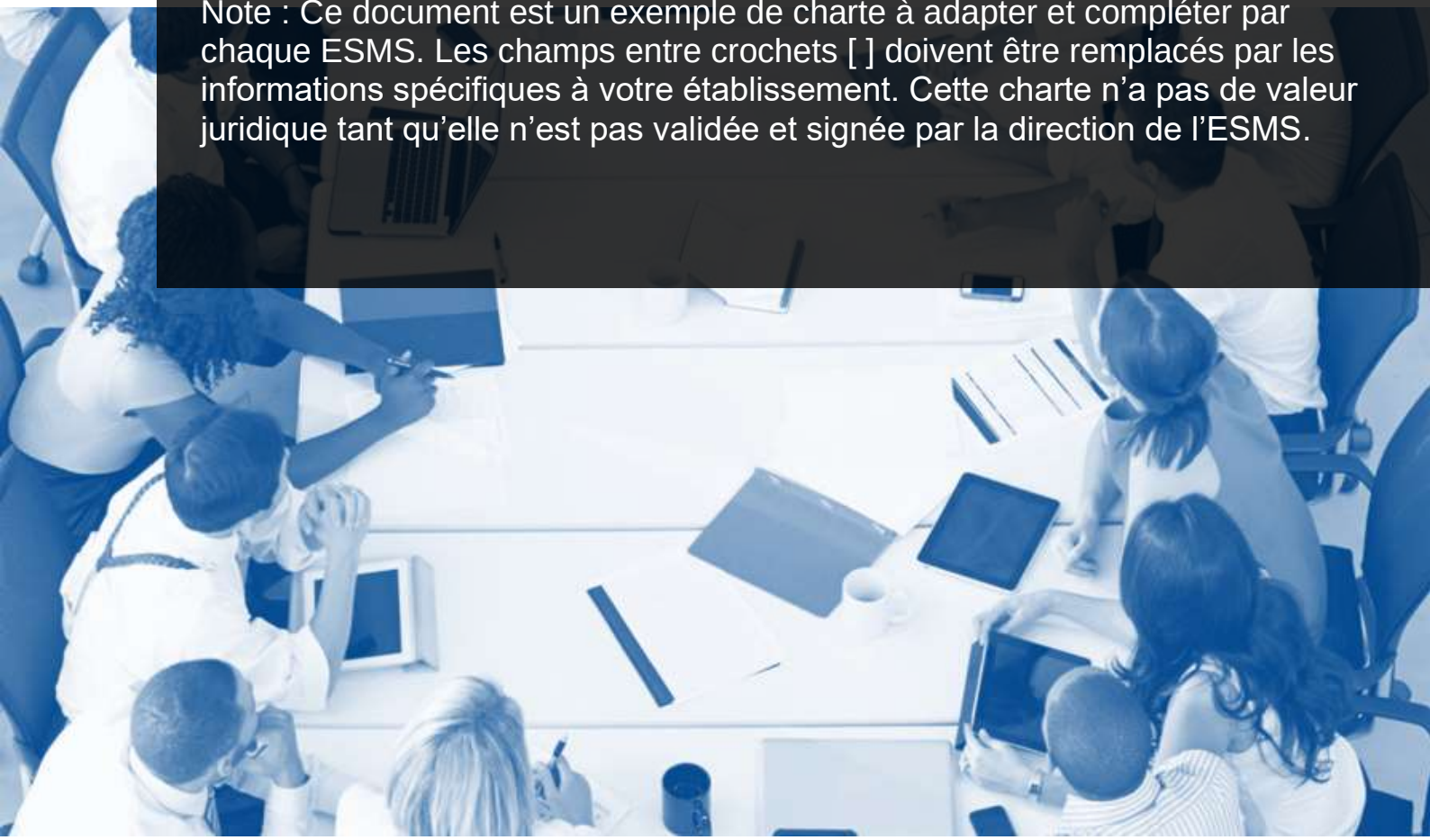

Table des matières

1 PREAMBULE 3
2 CHAMP D'APPLICATION DE CHARTE 3
3 DEFINITIONS 3
4 RAPPEL DU CADRE LEGISLATIF ET NORMATIF 4
5 AUTHENTIFICATION 4
5.1 PRESENTATION 4
5.2 REGLES D'USAGE 4
6 HABILITATIONS 5
6.1 PRESENTATION 5
6.2 REGLES D'USAGE 5
7 UTILISATION D'INTERNET ET DE LA MESSAGERIE 5
7.1 PRESENTATION 5
7.2 REGLES D'USAGE 6
8 PROTECTIONS DES DONNEES 6
8.1 PRESENTATION 6
8.1.1 Le RGPD 6
8.1.2 CNIL 7
8.1.3 IA-Act 7
8.2 REGLES D'USAGE 7
8.2.1 Accès aux données personnelles 7
8.2.2 Documents privés et professionnels 8
8.2.3 Utilisation de l'Intelligence Artificielle 8
9 UTILISATION DU MATERIEL INFORMATIQUE 8
9.1 PRESENTATION 8
9.2 REGLES D'USAGES 9
10 TELETRAVAIL ET DEPLACEMENTS PROFESSIONNELS 9
11 ABUS ET CONTROLS 9
12 INFORMATIONS A L'UTILISATEUR 10
12.1 PRISE DE MAIN ET MAINTENANCE A DISTANCE PAR LES TECHNICIENS INFORMATIQUES 10
12.2 ABSENCE DE L'UTILISATEUR 10
12.3 DEPART DE L'UTILISATEUR 10
12.4 PHOTOGRAPHIES, DROITS A L'IMAGE 11
13 REGLEMENTATION 11
13.1 RESPONSABILITES 11
13.2 LISTE DES TEXTES DE LOIS 11

1 Préambule

<ORGANISME GESTIONNAIRE> dispose d'un système d'information qui offre aux professionnels les moyens de collaborer et de communiquer ensemble. La présente charte définit les conditions d'accès et les règles d'utilisation des équipements mis à disposition.

Elle a également pour objectif de sensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes de confidentialité, de disponibilité, d'intégrité et de sécurité des données traitées.
Ces risques imposent le respect de certaines règles de bonne conduite. L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent en effet avoir de graves conséquences de nature à engager sa responsabilité civile et/ou pénale ainsi que celle de <ORGANISME GESTIONNAIRE>.

2 Champ d'application de charte

La présente Charte s'impose à tous les utilisateurs qui ont recours aux équipements numériques mis à disposition par <ORGANISME GESTIONNAIRE> pour l'exercice de leurs missions. Elle définit les droits et devoirs de chaque utilisateur. Sa signature conditionne l'accès aux systèmes d'information de l'Etablissement. Elle est remise en main propre à chaque salarié lors de son embauche. Elle est consultable à tout moment sur <LOCALISATION DU DOCUMENT>.

Ajouter : document opposable (annexé au règlement intérieur, signé) / cette charte est amenée à évoluer dans le temps

3 Définitions

On désignera de façon générale sous le terme :

- « Utilisateur » : la personne ayant accès ou utilisant les ressources informatiques, moyens téléphoniques et services internet quel que soit son statut.
- « Ressources informatiques », les postes de travail, les logiciels, ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade, à partir du réseau administré ou utilisé par <ORGANISME GESTIONNAIRE>.
- « Services Internet/Intranet » la mise à disposition par des serveurs locaux ou distants, de moyens d'échanges et d'informations diverses : site web, messagerie, application web.
- « Activité professionnelle » l'activité qui est nécessaire, utile, dépendante ou complémentaire à l'activité des services de <ORGANISME GESTIONNAIRE>, quelle qu'en soit la nature.
- « Moyens téléphoniques », tous les téléphones fixes, mobiles, mails ou fax, mis à disposition par <ORGANISME GESTIONNAIRE> pour l'exercice de l'activité professionnelle.
- « Service Informatique », l'équipe de professionnels (Interne ou Externe) qui œuvre au bon fonctionnement de l'ensemble des infrastructures du système d'information.
- « Personnes non salariées et visiteurs occasionnels » disposent de leur propre matériel et peuvent utiliser le WIFI <NOM DU WIFI INVITE> mise à disposition par <ORGANISME GESTIONNAIRE> pour se connecter sur internet, sans avoir recours au réseau professionnel de <ORGANISME PROFESSIONNEL>.

4 Rappel du cadre législatif et normatif

La charte s'inscrit dans :

- **RGPD** (Règlement Général sur la Protection des Données – UE 2016/679)
- **Code de la santé publique**
- **Code de l'action sociale et des familles (CASF)**
- **Code pénal** (articles 323-1 à 323-7 : atteintes aux STAD)
- **PGSSI-S (Politique Générale de Sécurité des Systèmes d'Information en Santé)** : référentiel national de sécurité en santé
- **Guide d'hygiène informatique de l'ANSSI**
- **IA Act** (règlement européen sur l'intelligence artificielle)

5 Authentification

5.1 Présentation

L'authentification est le processus qui permet de certifier l'identité d'une personne.

L'utilisateur devra s'authentifier pour se connecter au système d'information ou à ses applications métiers et protègera **son compte** à l'aide d'un mot de passe et d'un second facteur d'authentification.

Pour être valide, et conformément aux règles préconisées par l'ANSSI (Agence Nationale de la Sécurité du Système d'Information) un mot de passe devra nécessairement :

- Compter 12 caractères minimum ;
- Contenir trois de ces types de caractères : minuscule, majuscule, chiffre et caractère spécial ;
- Être renouvelé tous les ans ;
- Être différent des deux mots de passes précédents ;
- Ne pas faire mention du prénom ou du nom de l'utilisateur.

Le second facteur d'authentification sera : <A DEFINIR PAR l'OG>

L'utilisateur reconnait et accepte que son identifiant et son mot de passe constituent une identification électronique pour toute action menée au sein du système d'information. Il est considéré comme responsable de toutes actions réalisées à partir de son compte.

5.2 Règles d'usage

- Pour se protéger, l'utilisateur s'engage à :
- Ne jamais travailler sur le compte ou usurper l'identité d'un autre professionnel ;
- Conserver secret son mot de passe et avoir un mot de passe unique par usage ;
- Ne jamais communiquer son mot de passe à qui que ce soit (le service informatique n'en a pas besoin) ;
- Ne jamais écrire ses mots de passe sur aucun support accessible restant à proximité des ressources informatiques ;
- Verrouiller tout équipement (ordinateur, smartphone, etc…) dès que celui-ci n'est plus utilisé, y compris pour de courtes périodes ;
- Suivre l'ensemble des recommandations et règles communiquer par le service SI.

De manière générale, les mots de passe communs sont à limiter aux seules ressources de services (messagerie d'un service, guichet…),

6 Habilitations

6.1 Présentation

L'Habilitation est le processus qui permet d'attribuer des droits sur le Système d'Information en fonction du profil de l'utilisateur.

Un utilisateur est associé à un compte, un compte à un profil, un profil a des droits.

En fonction du poste occupé, chaque professionnel dispose de droits d'accès spécifiques au sein du système et des logiciels métiers qu'il utilise. Un changement de fonction peut impliquer des modifications (ajout, suppression) de certains droits d'accès.

Un droit est une responsabilité. Il est donc nécessaire de veiller à n'avoir que les droits nécessaires à l'exécution de ses missions.

Le responsable de traitements réalise périodiquement une revue des habilitations.

6.2 Règles d'usage

L'utilisateur s'engage à :

- Signaler au Service Informatique de <ORGANISME GESTIONNAIRE> tout dysfonctionnement ou violation (ou tentative de violation) de son compte réseau, ou accès à des ressources illégitimes (fichiers, répertoires, logiciels, fonctionnalités…) ;
- S'interdire l'accès à des ressources non nécessaires à l'exécution de sa mission ;
- Signaler à son responsable tout droit non nécessaire à l'exécution de sa mission.

7 Utilisation d'internet et de la messagerie

7.1 Présentation

L'usage des services Internet/Intranet et du réseau pour y accéder, ainsi que les moyens téléphoniques, sont mis à disposition des utilisateurs pour l'exercice des activités de <ORGANISME GESTIONNAIRE> ainsi qu'à ses prestataires, même occasionnels.

Toutefois, il est admis qu'un usage raisonnable des ressources à des fins personnelles puisse être toléré, à la condition expresse de respecter les dispositions de la présente charte. Cet usage personnel ne pourra être qu'occasionnel et limité, dans le temps et par son objet.

Un filtrage web est mis en place pour interdire aux utilisateurs l'accès aux sites pornographiques, aux messageries personnelles (webmail) et à tout site ou catégorie de sites pouvant s'avérer dangereux pour la sécurité et l'intégrité du Système d'information. Les traces de navigations sont conservées 6 minimum mois comme le mentionne les mesures de sécurité, de traçabilité et d'audit conformes à la PGSSI-E.

La messagerie est la porte d'entrée la plus simple pour un pirate informatique. La plus grande prudence est de mise lors de la réception d'un mail provenant d'un émetteur inconnu.

La quantité d'informations et leur facilité de circulation sur les services Internet/Intranet ne doivent pas faire oublier la nécessité de respecter la législation. Internet et les réseaux de communication numériques ne sont pas des zones de non droit. La transgression des règles d'usages pourrait donner lieu à des poursuites pénales.
L'utilisateur est informé que tout ~~abus~~ mésusage de l'utilisation non professionnelle des ressources informatiques pourra faire l'objet de sanctions disciplinaires.

7.2 Règles d'usage

Sur Internet comme sur la messagerie, l'utilisateur s'engage à :

- Ne pas porter atteinte à la vie privée d'autrui,
- Ne pas avoir de discours diffamatoire et injurieux,
- Ne pas inciter à la consommation de substances interdites,
- Ne pas faire promouvoir les crimes et délits, la discrimination, la haine notamment raciale ou à violence,
- Ne pas faire l'apologie des crimes notamment de meurtre, viol, crime de guerre et crime contre l'humanité ; la négation de crime contre l'humanité,
- Ne pas contrefaire des marques,
- Ne pas reproduire, représenter ou diffuser les œuvres musicales, photographies ou littéraires en violation des droits de l'auteur,
- Ne pas copier de logiciels commerciaux pour quelque usage que ce soit, hormis dans le cadre de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle ;

Dans le cadre de spécifique de l'usage de la messagerie, l'utilisateur s'engage à :

- Ne pas ouvrir de pièces jointes provenant d'émetteurs inconnus, ajouter une note sur les activités non concernées
- Ne pas suivre un lien dans un mail d'un émetteur inconnu sans s'être assuré de l'authenticité du site visé,
- Rester vigilant dans le traitement d'une demande urgente reçue par mail,
- Distinguer clairement les courriels qu'il considère comme personnels, des messages professionnels, notamment en les rangeant dans des dossiers distincts nommés « PERSONNEL », et/ou en faisant figurer « PERSONNEL » en objet des courriels. (Tout courriel ne respectant pas cette règle sera considéré comme professionnel et pourra être lu par une tierce personne notamment en cas de contrôle.
- Limiter le nombre de destinataires au strict minimum ;

En cas de doute, vous pouvez contacter votre service SI et/ou la personne concernée.

8 Protections des données

8.1 Présentation

8.1.1 Le RGPD

Le RGPD, définit les conditions dans lesquelles des traitements de données à caractère personnel doivent être mis en œuvre. Le RGPD augmente les droits des personnes concernées par les traitements de manière à leur redonner confiance et pouvoir agir sur leurs données. A ce titre, le principe de transparence, par une information claire et adaptée, est de rigueur.

<ORGANISME GESTIONNAIRE> peut désigner un délégué à la protection des données. Ce dernier veille à la correcte application et au respect du RGPD au sein des établissements et services de l'association, en collaboration avec le responsable des traitements. La sensibilité des données varient selon leur granularité : des données d'identification (peu sensibles) aux données de santé, considérées comme très sensibles.

Le délégué à la protection des données est en théorie consulté par la gouvernance de l'association, préalablement à la mise en œuvre de tout nouveau traitement.

Le délégué à la protection des donnés veille au respect des droits des personnes. En cas de difficultés rencontrées lors de l'exercice de ces droits, les personnes concernées peuvent l'alerter et le saisir directement via <METHODE DE SOLICITATION>.

8.1.2 CNIL

La CNIL (Commission Nationale de l'Informatique et des Liberté) garantit le respect de la vie privée en encadrant la collecte, le traitement et le stockage des données personnelles des personnes accompagnées. Ces dernières bénéficient de droits fondamentaux tels les droits d'accès et de rectification (liste non exhaustive cf CNIL).

Elle impose également des obligations aux organisations pour assurer la confidentialité, disponibilité, intégrité et sécurité des données, tout en veillant à ce que les utilisateurs soient informés de leurs droits et des usages faits de leurs informations.

8.1.3 IA-Act

L'IA Act est une réglementation européenne qui garantit la sécurité et la fiabilité des systèmes d'IA en imposant des règles strictes aux fournisseurs, notamment en matière de transparence et de gestion des risques. Les utilisateurs bénéficient ainsi d'une meilleure protection de leurs droits fondamentaux et d'une utilisation plus responsable et éthique de l'IA.

De plus, l'AI Act classe les systèmes d'IA selon leur niveau de risque, assurant que les applications à haut risque soient soumises à des obligations spécifiques pour minimiser les dangers potentiels.

8.2 Règles d'usage

8.2.1 Accès aux données personnelles

La gestion des données est assurée conformément à la Réglementation Générale sur le Protection des Données (RGPD), qui prévoit, pour toute personne, un droit d'accès aux données qui la concerne et à leur rectification. L'exercice de ce droit se fait par la voie hiérarchique.

L'utilisateur s'engage à :

- Respecter les consignes et mesures de sécurité logique, physique et organisationnelle communiquées par les directions de <ORGANISME GESTIONNAIRE> ou le DPO de l'association,
- Ne pas accéder ni tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas,
- Ne pas communiquer, hors messagerie sécurisé de santé, d'informations personnelles d'un tiers,
- Ne pas divulguer d'informations confidentielles, notamment par téléphone, à des tiers qui ne doivent pas les connaître,
- Déclarer au DPO tout fichier comportant des données personnelles et à en expliquer l'utilité,
- Rendre illisible ou mettre au rebus tout support papiers ou numérique (DVD/Clé USB) après usage ;

8.2.2 Documents privés et professionnels

L'utilisateur s'engage à :

- Distinguer clairement les documents, courriers, messages, etc… qu'il considère comme personnels, des documents professionnels, notamment en les rangeant dans des dossiers distincts nommés « PERSONNEL », et/ou en faisant figurer « PERSONNEL » en tête du nom des documents et de l'objet des courriels.
- Utiliser les serveurs de fichiers pour travailler de manière collaborative et pour protéger les données,
- Ne pas copier de données sur un support externe sans l'accord préalable de son supérieur hiérarchique ;
- Distinguer clairement les documents qu'il considère comme personnels, des documents professionnels, notamment en les rangeant dans des dossiers distincts nommés « PERSONNEL », et/ou en faisant figurer « PERSONNEL » en tête du nom des documents.
- Ne pas accéder aux données (lecture, modification, suppression) qui ne lui appartiennent pas sous peine d'être sanctionné pénalement ;
- Ne pas accéder aux données des usagers pour tout motif étranger à leur prise en charge,
- Ne pas diffuser des informations sur l'association ou ses usagers,
- Ne pas d'utiliser des photos de professionnelles ou d'usagers sans avoir recueilli leur consentement,
- Ne pas accéder à une correspondance (courriel) dont il n'est ni l'émetteur, ni le destinataire sans l'accord d'un des correspondants ;

8.2.3 Utilisation de l'Intelligence Artificielle

L'usage à l'intelligence Informatique doit être limité pour des raisons de consommation énergétique et d'impact sur l'environnement. Toutefois, celui-ci ne sera pas interdit. L'utilisation d'outil Français (MISTRAL IA) contraint par l'IA-Act est à privilégier.

Technologiquement, « L'IA génère du texte en **prédisant** le mot suivant dans une séquence, en se basant sur des modèles **statistiques** appris à partir de vastes ensembles de données. »
L'IA n'a donc aucune connaissance du sens de la phrase avant de la produire.

L'utilisateur s'engage à :

- N'utiliser que les IA soumises à la réglementation européenne IA-Act (MISTRAL IA par exemple)
- Valider scrupuleusement les réponses fournies par le moteur d'IA avant dans les intégrer dans un document professionnel ou dans un logiciel métier,
- Supprimer toute donnée personnelle (nom, prénom, numéro de téléphone, adresse, identifiant…) des questions posées à l'IA (toute requête doit être anonymisé) ;

L'IA doit être comme un assistant, toutes les informations doivent relue et vérifié

9 Utilisation du matériel informatique

9.1 Présentation

Les Ressources informatiques (Matériels informatiques, logiciels, espaces de stockages) sont mises à disposition de l'utilisateur dans la cadre de son activité professionnelle. Les droits d'accès sont régis par la matrice d'habilitation établie par la direction.

Tout utilisateur est responsable du bon usage des équipements mis à sa disposition. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale.

9.2 Règles d'usages

L'utilisateur s'engage à :

- Conserver les paramétrages et réglages du poste de travail effectués par le Service Informatique,
- Conserver l'installation des logiciels, propriété de <ORGNANISME GESTIONNAIRE>, à l'identique et ne pas chercher à en télécharger sans l'autorisation préalable de sa direction ou du service SI,
- Ne pas installer de logiciels non autorisés par le service SI,
- Conserver la configuration physique de l'installation du matériel et du réseau,
- Ne pas connecter au réseau ou déconnecter du réseau des périphériques informatiques et de communication non maîtrisée sans y avoir été autorisé par le service SI.
- Ne pas connecter de matériel personnel au réseau professionnel,
- Ne communiquer les mots de passe du WIFI interne aux intervenants externes ;
- Ne pas communiquer à des tiers des informations techniques concernant son matériel,
- Respecter le matériel mis à disposition, le protéger des liquides en tout genre et des chutes,

10 Télétravail et déplacements professionnels

L'utilisation des ressources informatiques de l'utilisateur, en situation de télétravail ou de déplacement professionnel doit respecter les mêmes règles de sécurité qu'au sein de l'établissement.

- **Connexion sécurisée obligatoire** via VPN ou réseau Wi-Fi sécurisé (interdiction des réseaux publics non sécurisés sans protection).
- Utilisation exclusive des **comptes professionnels** (messagerie, MSSanté, Pro Santé Connect).
- Les documents professionnels ne doivent pas être stockés localement sur l'équipement personnel ou portable sans autorisation expresse.
- Obligation de **verrouiller l'appareil** dès qu'il n'est pas utilisé, même pour une courte absence.
- En cas de perte ou vol du matériel (ordinateur, smartphone, clé USB), l'incident doit être déclaré immédiatement au RSSI ou à la direction.
- L'impression de documents contenant des données sensibles en dehors de l'établissement est interdite sauf autorisation préalable.

11 Abus et contrôls

L'utilisateur est informé que sa propre responsabilité, celle de son chef de service et la responsabilité de <ORGANISME GESTIONNAIRE> peuvent être engagées civilement et pénalement du fait de son comportement. Il veillera donc à respecter :

- Les lois et règlements en vigueur,
- Les règles d'utilisation, de sécurité et de bons usages décrits dans la présente charte ;

L'utilisateur est informé que

- Le système d'information de <ORGANISME GESTIONNAIRE> fait l'objet d'une surveillance automatique constante (serveurs, réseaux, postes de travail, téléphones, logiciel, virus…),
- Certains équipements sont soumis à une surveillance particulière, notamment sur les volumes d'informations traitées (enregistrement, téléchargement) qui analyse les durées d'utilisation, la nature de fichier stockés (films, photos, …), les connexions aux sites internet visités ou les tentatives d'intrusion,
- Que toutes ses actions sont tracées dans les logiciels métiers ;

En cas d'utilisation manifestement anormale d'un poste téléphonique (fixe ou mobile), un responsable de service peut demander au responsable des systèmes d'information, une facture détaillée masquant les 4 derniers chiffres des numéros composés.

12 Informations à l'utilisateur

12.1 Prise de main et maintenance à distance par les techniciens informatiques

Les techniciens informatiques de l'info-géreur disposent d'outils permettant d'accéder à n'importe quel poste de travail informatisé. Leur utilisation s'effectue en toute transparence et les données auxquelles le gestionnaire technique accède par ce moyen sont limitées au strict cadre de l'intervention.

Toute prise de main à distance nécessite l'information préalable et l'accord de l'utilisateur pour « donner la main » au technicien avant l'intervention sur son poste. L'utilisateur peut suivre sur son écran les manipulations faites par le technicien informatique.

12.2 Absence de l'utilisateur

En cas d'absence de l'utilisateur, la continuité du service doit être assurée. L'utilisateur doit veiller à ce que les membres de son service puissent accéder aux documents, logiciels et dossiers indispensables à l'activité professionnelle. Cela peut se faire par :

- la transmission directe des documents et dossiers aux collègues,
- la mise à disposition dans un dossier partagé,
- la création de comptes spécifiques pour accéder aux applications, **sans communiquer ses mots de passe personnels**.

Si l'absence est imprévue (maladie, accident), le supérieur hiérarchique peut, avec traçabilité, demander au service informatique l'accès aux documents professionnels de l'utilisateur. En cas de départ définitif ou de mutation, le successeur récupérera uniquement les documents de travail et les messages professionnels. Cette procédure respecte les règles définies au paragraphe 5.2 « Documents privés et professionnels ».

12.3 Départ de l'utilisateur

Lors de son départ, l'utilisateur doit supprimer **tous les mails personnels** de sa messagerie professionnelle. Il est informé que la messagerie professionnelle pourra être supprimée ou partagée avec ses collègues et responsables **uniquement pour les besoins de continuité du service**. Cette mesure ne remet pas en cause l'interdiction de consulter les mails explicitement marqués comme personnels.

- Quelle qu'en soit la raison (fin de contrat, démission, mutation, retraite) :
- L'utilisateur doit restituer **l'ensemble du matériel professionnel** mis à sa disposition (ordinateur, téléphone, badge d'accès, clé USB, cartes d'authentification, etc.).
- Aucun équipement ou support contenant des données professionnelles **ne peut être conservé à titre personnel**.
- L'<ORGANISME GESTIONNAIRE> procède **immédiatement à la désactivation des accès informatiques** (messagerie, MSSanté, Pro Santé Connect, VPN, etc.).
- Le collaborateur s'engage à effacer de ses équipements personnels **toutes données liées à son activité professionnelle**, dans le respect des règles RGPD et sécurité interne.
- Un inventaire de restitution pourra être réalisé par la direction ou le service informatique **avec signature ou traçabilité**, pour garantir le retour complet du matériel et des données.
-

Tout manquement à ces obligations pourra entraîner **des mesures disciplinaires et, le cas échéant, des poursuites judiciaires**.

12.4 Photographies, droits à l'image

L'image d'une personne ne peut être utilisée ou diffusée sans son consentement écrit (celui de son responsable légal pour un mineur). D'une manière générale, les photos que les utilisateurs peuvent être amenés à prendre dans l'exercice de leurs fonctions ne doivent donc pas comporter de personnes, plaques d'immatriculation, enseignes de magasins étrangères à l'affaire : il est recommandé de flouter ces éléments.
Les photos prises dans le cadre des activités de <ORGANISME GESTIONNAIRE> ne peuvent pas être utilisées à ses fins personnelles, et sont interdites à la diffusion externe sans le consentement écrit de la Direction Générale. Cette recommandation s'applique également aux enregistrements vidéo et sonores.

13 Réglementation

13.1 Responsabilités

L'utilisateur est informé que sa propre responsabilité, celle de son chef de service et la responsabilité de <ORGANISME GESTIONNAIRE> peuvent être engagées civilement et pénalement du fait de son comportement. Il veillera donc à respecter :

- Les lois et règlements en vigueur, notamment ceux mentionnés à l'article 6.2,
- Les règles d'utilisation, de sécurité et de bons usages décrits dans la présente charte ;

13.2 Liste des textes de lois

Le présent article a pour objectif d'informer les utilisateurs des principaux textes législatifs et réglementaires définissant notamment les droits et obligations des personnes utilisant les ressources informatiques. Il ne s'agit en aucune manière d'une liste exhaustive :

Loi n° 78-17 du 6 janvier 1978, modifiée, relative à l'informatique, aux fichiers aux libertés, qui a notamment pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'utilisation de l'informatique et d'encadrer l'utilisation des données à caractère personnel dans les traitements informatiques.

Loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications.
Code Pénal, pris notamment en ses articles 323-1 à 323-7 visant les atteintes aux systèmes de traitement automatisé des données.

Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

L'ordonnance N°2005-1516 du 8 décembre 2005, relatives aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives permet notamment à une administration de répondre par voie électronique à une demande d'information d'un usager ou d'une autre administration qui lui a été adressée par la même voie, et prévoit que les actes et administrations peuvent être signés électroniquement pour assurer l'identification signataire et l'intégrité des actes.

Code de la Propriété. Intellectuelle. Il reconnaît les logiciels comme œuvres de l'esprit, et à ce titre, ils sont protégés sans nécessiter de dépôt ou d'enregistrement.

Code du patrimoine, pris notamment en ses articles L211-1 à L211-4. Il définit les archives comme étant l'ensemble des documents, quels que soient leur date, leur forme et leur support matériel, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité. Les archives publiques sont notamment les documents qui procèdent de l'activité des collectivités territoriales.
Loi n°94-665du 4 août 1994 modifiée, relative à l'emploi de la langue française. Elle prévoit, lorsqu'ils existent, l'emploi de termes français de même sens en lieu et place des termes étrangers.