MODELE DE CHARTE INFORMATIQUE

[LOGO DE LA CPTS]

Charte informatique de la
[NOM DE LA CPTS …]

Préambule :
L'élaboration d'une charte d'utilisation des moyens informatiques et sa mise à disposition auprès des utilisateurs figure parmi les bonnes pratiques à mettre en œuvre dans toute entité dont les informations, données et activités s'appuient sur un système d'information.

Les attaques informatiques n'ont de cesse de progresser en nombre, en efficacité et en complexité avec des conséquences telles que l'atteinte à l'image, l'indisponibilité et la divulgation de données.

Mais la transition numérique est également porteuse de formidables opportunités dès lors que des mesures de sécurité numérique sont mises en place.

Cette charte établit des règles claires pour l'utilisation des technologies de l'information par tous les membres de notre CPTS, incluant les salariés et les professionnels de santé. Chacun est invité à adhérer à ces directives pour garantir la sécurité de nos systèmes et la confidentialité des données que nous gérons.

1. Utilisation des équipements informatiques

Principe général :

Tous les équipements informatiques et logiciels fournis par la CPTS sont exclusivement destinés à des fins professionnelles.

Directives spécifiques :

Séparation des usages : Utilisez des appareils et des comptes distincts pour vos activités professionnelles et personnelles afin d'éviter toute interférence ou compromission de données.

Accès autorisé : Ne permettez à personne d'utiliser votre équipement dans le cadre de votre activité professionnelle sans autorisation préalable

2. Sécuriser l'accès au compte

Chaque utilisateur est responsable de la sécurité de ses identifiants d'accès et ne doit pas les divulguer à des tiers. Cette identification permet, à chaque connexion, l'attribution de droits et privilèges propres à chaque utilisateur sur les ressources du système dont il a besoin pour son activité.

Une identification (login + mot de passe) est unique à chaque utilisateur. Ce dernier est personnellement responsable de l'utilisation qui peut en être faite, et ne doit en aucun cas la communiquer.

Mesures à suivre :

Changez régulièrement votre mot de passe conformément à notre politique (à déterminer) et après la déclaration d'un incident malveillant.

Créez des mots de passe forts, qui ne doivent pas être facilement devinables (évitez les noms, dates de naissance, etc.).

3. Sécurité des données

La sécurité des données est une responsabilité partagée. Chaque utilisateur doit prendre des mesures pour protéger les informations auxquelles il a accès.
Tout salarié et tout adhérent est responsable de la sécurité des données auxquelles il accède ou qu'il traite.

Directives importantes :

Confidentialité : Ne divulguez jamais les données de santé des patients sans autorisation explicite.

Stockage sécurisé : Conformez-vous aux principes du RGPD, en veillant à ce que les données soient stockées et traitées de manière sécurisée.

[Rappelez les principes du RGPD essentielles à respecter]

Les données des patients ne doivent être accessibles qu'aux membres de la CPTS autorisés à les consulter dans le cadre de leur travail. Il est interdit de partager des données sensibles avec des tiers non autorisés.

[Les dispositifs de stockage amovibles (clés USB, disques durs externes, etc.) ne doivent être utilisés que conformément aux politiques de sécurité de la CPTS, et leur utilisation pour stocker des données sensibles est strictement interdite sauf autorisation expresse]

4. Utilisation d'Internet et des e-mails

L'accès à Internet et l'usage des e-mails doivent être réalisés avec prudence et dans le respect total de la confidentialité et de la sécurité des données de la CPTS.

Chaque utilisateur doit prendre conscience qu'il est dangereux pour la CPTS :
- de communiquer à des tiers des informations concernant son matériel et son activité ;
- de diffuser des informations de la CPTS via des sites Internet ;
- de participer à des forums *(même professionnels)* ;
- de participer à des conversations en ligne (« chat ») ;
- de cliquer sur des liens malveillants ;
- …

Les e-mails professionnels doivent être utilisés de manière responsable et respecter les politiques de confidentialité. Il ne doit pas être envoyé de mails contenant des informations confidentielles à :
- des destinataires non autorisés ;
- des destinataires autorisés sur une messagerie non sécurisée [*Exemple : …]*

Il est interdit de partager des données de santé ou données sensibles en dehors des canaux sécurisés. En conséquence, toute donnée sensible doit être échangée de manière sécurisée.
[Précisez les outils collaboratifs sécurisés. Exemple : Medimail, SPICO discussions, MSS ….]

Bonnes pratiques :

Utilisez Internet uniquement pour des activités qui soutiennent les objectifs de la CPTS.

Ne partagez pas d'informations professionnelles sur des forums publics ou des réseaux sociaux sans sécurisation et autorisation.

5. Sécurité informatique

Tous les utilisateurs sont tenus de prendre des mesures raisonnables pour protéger les systèmes informatiques de la CPTS contre les menaces de sécurité, y compris les virus, les logiciels malveillants et les tentatives d'accès non autorisées.
La mise à jour régulière des systèmes et applications ainsi que de l'antivirus sont à faire dès que possible.

[Il est recommandé d'activer l'application des mises à jour automatiques]

Les utilisateurs doivent signaler toute suspicion d'incident de sécurité ou de violation de données à l'administrateur informatique de la CPTS [Nom et coordonnées] dès que possible.

6. Sauvegardes

La mise en œuvre du système de sécurité *[ne]* comporte [*pas]* des dispositifs de sauvegarde des informations destiné à doubler le système en cas de défaillance.
[A définir avec votre prestataire informatique et chaque sous-traitant]

Une sauvegarde est à réaliser sur un support dématérialisé [X fois par mois / trimestre].

7. Utilisation responsable

Tout salarié et membre de la CPTS est responsable de respecter les dispositions de cette charte informatique et d'en diffuser les usages auprès des adhérents de la CPTS.

Les systèmes informatiques de la CPTS ne doivent pas être utilisés pour accéder à du contenu illicite, inapproprié ou offensant, ni pour mener des activités personnelles non liées au travail.

L'utilisation des ressources informatiques de la CPTS pour diffuser des informations confidentielles ou sensibles en dehors de la CPTS est strictement interdite.

[La CPTS s'engage à sensibiliser et former ses adhérents aux bonnes pratiques en matière de sécurité informatique et de protection des données, afin de prévenir les risques de violation de la confidentialité]

Fait à [...], le [...]
Signature du Président de CPTS