| MODÈLE DE CHARTE D'UTILISATION DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION DE [Nom de l'Établissement de Santé] |
| --- |

| Version |  |
| --- | --- |
| Classification |  |
| Diffusion |  |

| Cycle de vie du document |
| --- |
| **Date** | **Révision** | **Rédacteur** | **Note** |
| 00/00/2025 | 1.0 | Prénom Nom | Création du document |
|  |  |  |  |

| **Voici un modèle de charte informatique adapté au contexte d'un établissement sanitaires et médico-sociauxen France. Ce modèle est une base et doit impérativement être adapté et validé par les services juridiques et la direction de votre établissement, en tenant compte de votre organisation spécifique, de vos systèmes d'information et des dernières évolutions légales (notamment RGPD, Code de la Santé Publique, jurisprudence).****L'aspect crucial dans le domaine sanitaire et médico-socialest la confidentialité des données patients ou usagers et le secret médical. Ces points doivent être au cœur de la charte.****Adaptations nécessaires :*** **Personnalisation :** Remplacer les crochets [Nom de l'Établissement] par le nom réel.
* **Contact IT/Sécurité :** Préciser qui contacter en cas de problème (Service informatique, RSSI - Responsable Sécurité des Systèmes d'Information, DPO - Délégué à la Protection des Données).
* **Règles spécifiques :** Ajouter des règles propres à votre établissement (ex: utilisation des tablettes en chambre, règles spécifiques pour la télémédecine, utilisation de logiciels métiers particuliers).
* **Références légales internes :** Mentionner le règlement intérieur ou les procédures disciplinaires de l'établissement.
* **Glossaire :** Il peut être utile d'ajouter un glossaire définissant les termes techniques ou légaux (RGPD, DPI, HDS, phishing, etc.).
* **Document d'accusé réception :** Prévoir un formulaire que chaque utilisateur doit signer pour attester avoir reçu et compris la charte.
* **Validation Juridique :** C'est l'étape la plus importante. Faites relire ce document par un juriste spécialisé en droit de la santé et en droit du numérique.

Ce modèle vous donne une structure solide et couvre les points essentiels pour un établissement sanitaire ou médico-social. N'oubliez pas de l'adapter finement à votre contexte spécifique. |
| --- |

**MODÈLE DE CHARTE D'UTILISATION DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION** **DE [Nom de l'Établissement sanitaire ou médico-social]**

**Préambule**

Les systèmes d'information et de communication (SIC) sont essentiels au bon fonctionnement de [Nom de l'établissement], à la qualité des soins et à la gestion administrative. Ils permettent le partage d'informations, l'accès à des ressources documentaires, la communication interne et externe, ainsi que l'utilisation d'applications métiers spécifiques (Dossier Patient Informatisé - DPI, logiciels de laboratoire, de radiologie, Dossier Usager Informatisé (DUI),etc.).

L'utilisation de ces outils impose des règles strictes, particulièrement dans le secteur sanitaire ou médico-social où la confidentialité, l'intégrité et la disponibilité des données, notamment des données à caractère personnel sensibles, sont primordiales et protégées par la loi (secret professionnel, secret médical, RGPD, etc.).

La présente charte a pour objet de définir les règles d'utilisation des SIC de [Nom de l'établissement], les droits et devoirs de chaque utilisateur, afin de garantir la sécurité, la confidentialité et le bon usage des ressources mises à disposition.

[**Article 1 : Objet et Champ d'Application 6**](#_p4oaezyylgsp)

[1.1. Objet : 6](#_m83n7va9aqm0)

[1.2. Champ d'Application : 6](#_cgrb31hyxtof)

[**Article 2 : Acceptation de la charte 6**](#_z246ol6fggsz)

[**Article 3 : Accès aux Systèmes d'Information 6**](#_kp93vi3zsnt)

[3.1. Comptes utilisateurs et mots de passe : 6](#_6t2xre9xamvo)

[3.2. Fin d'accès aux SIC : 6](#_3yz4gwf1uqhn)

[**Article 4 : Utilisation des ressources informatiques 7**](#_2rp6bsz0g2gg)

[4.1. Principes généraux : 7](#_34gt1f57099n)

[4.2. Matériels : 7](#_ly6blvisv4h)

[4.3. Logiciels : 7](#_kny1u338sxz1)

[**Article 5 : Utilisation d'Internet et de la Messagerie Électronique 7**](#_rr39ddbs9ocr)

[5.1. Accès Internet : 7](#_v87ng5cikzyo)

[5.2. Messagerie électronique professionnelle : 8](#_vr6rl6bt2z8x)

[**Article 6 : Confidentialité et Protection des Données (Focus Santé) 8**](#_jgflwu2k8c2m)

[6.1. Secret professionnel et secret médical : 8](#_hx0utratj499)

[6.2. Protection des données personnelles (RGPD) : 8](#_6vfzfj27k8zt)

[6.3. Sécurité des postes de travail : 8](#_xtmb2imzsygr)

[**Article 7 : Sécurité des Systèmes d'Information 8**](#_anzpkufhyfu5)

[7.1. Protection contre les menaces : 9](#_tmk52mlsv704)

[7.2. Signalement d'incidents : 9](#_gli92xn3uksf)

[**Article 8 : Contrôle et surveillance de sécurité 9**](#_em5pxwmm0nj8)

[**Article 9 : Non-respect de la charte et sanctions 9**](#_5fd1lcppiiu7)

[Article 10 : Engagements individuels en matière de sécurité : 9](#_4du8q2lgqpx1)

[**Article 11 : Révision de la charte 10**](#_qhgvbenfv2wp)

[**Article 12 : Prise d'effet 10**](#_2y5istsl0rso)

# Article 1 : Objet et Champ d'Application

## 1.1. Objet :

Définir les règles d'accès et d'utilisation des systèmes d'information et de communication de [Nom de l'Établissement].

## 1.2. **Champ d'Application :**

La présente charte s'applique à toute personne accédant ou utilisant, à titre professionnel ou autre, tout ou partie des SIC de [Nom de l'Établissement]. Cela inclut, sans s'y limiter :

* Le personnel salarié (médical, paramédical, administratif, technique, etc.)
* Les médecins libéraux intervenant dans l'établissement
* Les stagiaires
* Les prestataires externes et intervenants temporaires
* Toute personne ayant accès aux locaux ou aux équipements informatiques de l'établissement.

# Article 2 : Acceptation de la charte

Tout utilisateur des SIC de l'établissement est réputé avoir pris connaissance de la présente charte et s'engage à en respecter les termes. L'accès aux ressources informatiques peut être conditionné à la signature d'un document attestant de cette prise de connaissance et de cet engagement.

# Article 3 : Accès aux Systèmes d'Information

## 3.1. **Comptes utilisateurs et mots de passe :**

* Chaque utilisateur se voit attribuer un compte personnel et unique.
* Le mot de passe associé est strictement personnel et confidentiel. Il ne doit en aucun cas être communiqué à un tiers, y compris à un membre du service informatique.
* Les utilisateurs sont responsables de la sécurité de leur mot de passe et de toutes les actions effectuées avec leur compte.
* Il est recommandé d’utiliser un mot de passe différent pour chaque application ou service. L’utilisation d’un seul mot de passe pour tous les accès est fortement déconseillée.
* Les mots de passe doivent respecter les règles de complexité et de renouvellement définies par la direction ou son représentant chargé de la gestion des systèmes d’information..

## 3.2. **Fin d'accès aux SIC :**

L'accès aux SIC est retiré automatiquement (ou dans les plus brefs délais) en cas de départ de l'établissement (fin de contrat, départ à la retraite, fin de stage, etc.) ou en cas de non-respect grave des règles établies.

Lors de son départ de la structure, l’utilisateur doit restituer au service informatique l’ensemble des équipements, supports ou documents numériques qui lui ont été confiés : ordinateurs, téléphones, clés USB professionnels, badges, etc.

Avant cette restitution :

* l’utilisateur est tenu de supprimer l’ensemble de ses fichiers et données personnels ou privés figurant sur les équipements ;
* aucune copie de documents ou données professionnelles ne peut être effectuée ou conservée par le collaborateur, sauf autorisation expresse de la direction de la structure.

Les comptes utilisateurs et les données personnelles associées sont supprimés dans un délai maximum d’un mois après le départ, sauf obligation légale de conservation spécifique.

# Article 4 : Utilisation des ressources informatiques

## 4.1. **Principes généraux :**

* Les SIC (postes de travail, applications logicielles, réseau, accès internet, messagerie électronique, etc.) sont mis à disposition dans un cadre strictement professionnel.
* Une utilisation raisonnable et limitée à des fins personnelles peut être tolérée, dans la mesure où elle ne nuit pas à l'activité professionnelle, ne compromet pas la sécurité des systèmes, ne génère pas de coûts excessifs pour l'établissement et respecte la législation en vigueur.
* Il est important de séparer la sphère professionnelle de la sphère personnelle : il est ainsi interdit de stocker des fichiers de l’établissement sur des comptes personnels (Google Drive, Dropbox, etc.), et d’utiliser des comptes professionnels pour des usages privés.

## 4.2. **Matériels :**

* Le matériel informatique (ordinateurs fixes ou portables, tablettes, smartphones professionnels, imprimantes, scanners, etc.) est la propriété de l'établissement.
* Il doit être utilisé avec soin et dans le respect des consignes d'utilisation.
* Il est interdit de modifier la configuration matérielle ou logicielle du poste de travail sans autorisation du service informatique.
* Le raccordement de matériels personnels (ordinateurs portables, disques durs externes, clés USB) aux systèmes de l'établissement est strictement réglementé et peut être interdit pour des raisons de sécurité. Seuls les dispositifs autorisés par le service informatique peuvent être utilisés.
* En cas de déplacement, les équipements sont sous la responsabilité de l’utilisateur et doivent être transportés et stockés avec précaution, dans des lieux sûrs et fermés à clé lorsque possible.

## 4.3. **Logiciels :**

* Seuls les logiciels installés et gérés par le service informatique sont autorisés.
* Il est strictement interdit d'installer ou de désinstaller un logiciel sans l'accord préalable de la direction ou de son représentant chargé de la gestion des systèmes d’information..
* L'utilisation de logiciels doit respecter les licences d'utilisation dont dispose l'établissement.

# Article 5 : Utilisation d'Internet et de la Messagerie Électronique

## 5.1. **Accès Internet :**

* L'accès à internet est fourni dans un cadre professionnel.
* Il est strictement interdit de consulter des sites à caractère illégal, violent, pornographique, discriminatoire, ou incitant à la haine raciale ou religieuse.
* Le téléchargement de fichiers (logiciels, musique, vidéos, etc.) non lié à l'activité professionnelle est interdit car il peut compromettre la sécurité.

## 5.2. **Messagerie électronique professionnelle :**

* La messagerie électronique est un outil de communication professionnelle.
* Il est interdit d'envoyer des messages à caractère illégal, insultant, diffamatoire, discriminatoire, ou de propager des rumeurs ou des informations non vérifiées.
* L'envoi de messages en masse (spam) ou la participation à des chaînes de lettres sont interdits.
* Les courriels, même identifiés comme "personnels", envoyés et reçus via la messagerie professionnelle sont, dans certaines limites légales, susceptibles de contrôle par l'employeur. Il est donc fortement recommandé de dissocier l'usage professionnel de l'usage personnel.
* Il est interdit d’utiliser son compte de messagerie professionnelle pour s’inscrire à des services personnels.

# Article 6 : Confidentialité et Protection des Données (Focus Santé)

## 6.1. **Secret professionnel et secret médical :**

* Tout le personnel est soumis au secret professionnel et, pour le personnel soignant, au secret médical, conformément à la loi. L'accès aux données de santé des patients ou usagers via les SIC est particulièrement protégé.
* L'accès aux informations contenues dans les systèmes (DPI, DUI, résultats d'examens, données administratives patients, etc.) est strictement limité aux informations nécessaires à l'exercice des fonctions de l'utilisateur (principe du "besoin d'en connaître").
* Il est formellement interdit de consulter les données de santé de patients sans lien direct avec sa prise en charge ou son suivi par l'utilisateur dans le cadre de ses fonctions.
* Les données de santé ne doivent jamais être divulguées à des personnes non autorisées, ni consultées dans un lieu où elles pourraient être vues par des tiers (espaces publics, transports, etc.).

## 6.2. **Protection des données personnelles (RGPD) :**

* Les utilisateurs doivent respecter scrupuleusement les principes du Règlement Général sur la Protection des Données (RGPD), en particulier concernant les "données de santé" qui sont des données sensibles.
* Il est interdit de copier, stocker ou transférer des données patients sur des supports non sécurisés ou personnels (clés USB personnelles, disques durs externes personnels, cloud non autorisé, messageries personnelles).
* Toute manipulation de données de santé (consultation, modification, suppression, impression) doit être justifiée par l'activité professionnelle et traçable.
* En cas de doute sur le traitement d'une donnée, l'utilisateur doit se rapprocher de son responsable hiérarchique ou du Délégué à la Protection des Données (DPO) de l'établissement.

## 6.3. **Sécurité des postes de travail :**

* Les utilisateurs doivent verrouiller leur session (Windows + L ou équivalent) dès qu'ils s'absentent de leur poste de travail, même pour une courte durée. Cela empêche l'accès non autorisé aux données et applications, y compris le DPI ou le DUI.
* Ne laisser traîner aucun document papier contenant des données confidentielles à proximité du poste de travail.

# Article 7 : Sécurité des Systèmes d'Information

## 7.1. **Protection contre les menaces :**

* Les utilisateurs doivent être vigilants face aux tentatives de fraude (phishing, hameçonnage) et aux logiciels malveillants.
* Ne jamais ouvrir de pièce jointe ou cliquer sur un lien dans un courriel d'expéditeur inconnu ou suspect.
* Ne jamais brancher de périphérique USB d'origine douteuse.

## 7.2. **Signalement d'incidents :**

Chaque collaborateur a le devoir de signaler immédiatement tout dysfonctionnement, anomalie ou incident de sécurité constaté dans l’usage des équipements informatiques ou dans le traitement des données.

Cela inclut notamment :

* toute tentative d'intrusion dans le système (accès suspect, connexion inhabituelle, etc.) ;
* toute altération ou modification inattendue de fichiers, programmes ou données ;
* tout acte de destruction volontaire ou accidentelle d'informations ou de documents numériques ;
* la perte ou le vol d’un équipement contenant des données professionnelles ;
* l'ouverture par erreur d’un courriel suspect, ou d’une pièce jointe ou d’un lien potentiellement malveillant.

Le signalement doit être fait sans délai à la direction de la structure ou à son représentant chargé de la gestion des systèmes d’information, même si l’incident paraît mineur ou sans conséquence apparente.

L’objectif de cette obligation est de protéger l’intégrité du système d'information, de prévenir la propagation d’éventuels dommages et de respecter les obligations légales en matière de sécurité et de protection des données. Aucune sanction ne sera prise contre un collaborateur qui signale de bonne foi une erreur ou une négligence.

# Article 8 : Contrôle et surveillance de sécurité

L'établissement se réserve le droit de contrôler l'utilisation des SIC, conformément à la législation en vigueur (Code du Travail, lois sur la protection des données), afin de garantir la sécurité des systèmes, le respect de la présente charte et des lois. Ces contrôles sont effectués dans le respect de la vie privée des utilisateurs et de la réglementation sur la protection des données personnelles.

# Article 9 : Non-respect de la charte et sanctions

Tout manquement aux règles énoncées dans la présente charte constitue une faute et expose l'utilisateur à des sanctions disciplinaires, pouvant aller jusqu'au licenciement. En fonction de la gravité du manquement, et notamment en cas de violation du secret médical ou de la réglementation sur la protection des données, l'utilisateur s'expose également à des poursuites pénales et civiles (amendes, peines de prison).

# Article 10 : Engagements individuels en matière de sécurité :

Tout utilisateur s’engage à respecter les règles de sécurité suivantes, essentielles à la protection des systèmes d'information de la structure :

* Signaler à la direction ou à son représentant chargé de la gestion des systèmes d’information toute violation ou tentative de violation suspectée de son compte réseau, ainsi que tout dysfonctionnement ou comportement inhabituel.
* Ne jamais confier son identifiant ou son mot de passe à qui que ce soit.
* Ne jamais demander à un collègue ou collaborateur de lui fournir son identifiant ou mot de passe.
* Ne pas masquer sa véritable identité lorsqu’il utilise un service ou un outil numérique de l’entreprise.
* Ne pas usurper l'identité d'un autre utilisateur.
* Ne pas modifier les paramétrages de son poste de travail sans autorisation préalable de la direction ou de son représentant chargé de la gestion des systèmes d’information.
* Ne pas installer de logiciels sans validation ou autorisation de la direction ou de son représentant chargé de la gestion des systèmes d’information.
* Verrouiller son ordinateur dès qu’il quitte son poste de travail, même pour une courte durée.
* Ne pas accéder, tenter d’accéder, modifier ou supprimer des informations qui ne relèvent pas de son périmètre d’activité ou de responsabilité.
* Ne pas copier ou transférer de données professionnelles sur un support externe sauf accord exprès de la direction ou de son représentant chargé de la gestion des systèmes d’information.

Les visiteurs ou prestataires extérieurs ne peuvent accéder aux outils informatiques ou de communication de la structure qu’avec l’accord préalable de la direction ou de son représentant chargé de la gestion des systèmes d’information. Dans ce cas, ils doivent s’engager à respecter cette charte, et à en faire respecter les dispositions par leurs propres salariés ou intervenants.

# Article 11 : Révision de la charte

La présente charte pourra être modifiée ou complétée par l'établissement en fonction de l'évolution des techniques, de l'organisation, de la législation et des risques identifiés.

# Article 12 : Prise d'effet

La présente charte prend effet à compter de sa date de diffusion.

Elle doit être lue et approuvée par chaque membre du personnel, qui s'engage à en respecter les termes.