



Royaume du Maroc
Ministère de la Santé
et de la Protection Sociale
Centre Hospitalo-Universitaire Hassan II

المركز الاستشفائي الجامعي الحسن الثاني - فاس
CENTRE HOSPITALO-UNIVERSITAIRE HASSAN II - FES

المملكة المغربية
وزارة الصحة والحماية الاجتماعية
المركز الاستشفائي الجامعي الحسن الثاني
CENTRE HOSPITALO-UNIVERSITAIRE HASSAN II - FES



CHARTRE D'UTILISATION DES RESSOURCES INFORMATIQUES

Version 1



Note de présentation

Dans le cadre de l'engagement continu et proactif envers la sécurité des informations et la conformité réglementaire, la présente Charte d'Utilisation des Ressources Informatiques établit les bonnes pratiques et procédures destinées à assurer l'utilisation sécurisée et efficace des technologies de l'information au sein du Centre Hospitalo-Universitaire Hassan II de Fès. Cette Charte est conçue pour protéger à la fois les ressources informatiques et les données sensibles gérées par l'établissement, tout en respectant les dispositions légales du Royaume du Maroc en matière de lutte contre la cybercriminalité, en outre, les exigences de la Directive Nationale de la Sécurité des Systèmes d'Information (DNSSI) ainsi que le règlement intérieur du CHU.

En effet, la législation marocaine relative à la cybercriminalité, y compris la loi n°05-20 et la loi n°08-09 qui modifie et complète le Code pénal par des dispositions relatives aux systèmes de traitement automatisé des données, et la directive nationale de la sécurité des systèmes d'information (DNSSI), ainsi que l'article 129 du règlement intérieur du centre hospitalo-universitaire Hassan II, serrent de fondement juridique et réglementaire à cette Charte. Elles définissent clairement les comportements illicites et les sanctions associées, encadrants ainsi l'utilisation des ressources informatiques de manière à prévenir toute activité susceptible de constituer une infraction.

En adhérant à ces lois, le CHU Hassan II assure que les utilisateurs des ressources informatiques sont bien informés de leurs responsabilités et des conséquences légales de leurs actions concernant les ressources informatiques de l'établissement.



Table des matières

I. But et objet.....	3
II. Champ d'application	3
III. Définitions et abréviations.....	3
IV. Description de la charte	3
V. Nature juridique de la charte.....	4
VI. Énoncé de la charte.....	4
1. Porté et responsabilité	4
2. Sécurité du système d'information.....	6
3. Droit d'accès	7
4. Confidentialité des données.....	8
5. Protection des données à caractère personnel	8
6. Sauvegarde des données.....	8
7. Usage de la messagerie :.....	9
8. Mesures de sécurité pour les terminaux nomades.....	10
9. Gestion des supports amovibles	10
10. Gestion des téléphones :.....	11
11. Gestion des points d'accès :	11
12. Gestion des accès à distance :	11
13. Analyse et contrôle de l'utilisation du système informatique :.....	11
14. Utilisation Internet :	12
15. Activités interdites :	12
16. Révision de la charte.....	13
17. Entrée en vigueur.....	13



V. Nature juridique de la charte

La présente précise les dispositions, auxquelles tout utilisateur doit se conformer, s'ajoutent aux textes de lois et règlements en vigueur et notamment ceux cités ci-dessous à titre énonciatif et non limitatif :

- Loi 05-20 : complétant le code pénal en ce qui concerne la cyber sécurité ;
- Loi 07-03 : complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données publiées au Bulletin Officiel n° 5184 du 5 février 2004 ;
- Loi 53-05 : relative à l'échange électronique de données juridiques qui précise les règles liées à l'utilisation de moyens cryptographiques pour l'échange de données ;
- Loi 09-08 : relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel publiées au Bulletin Officiel n° 5744 du 18 Juin 2009;
- La loi n°2-00 : portant promulgation relative aux droits d'auteur et droits voisins.

VI. Énoncé de la charte

1. Porté et responsabilité

La présente charte s'applique à tout utilisateur du système informatique du CHUHII. Chaque utilisateur, ayant accès au système informatique, est censé avoir pris acte de son engagement à l'utiliser dans un cadre professionnel.

➤ Responsabilité du personnel

Le personnel du CHUHII utilisant un poste de travail (PCs, Portable, ...) est responsable de ce qui suit :

- La protection de toutes les informations professionnelles installées dans son poste de travail et plus particulièrement des données à caractère personnel qu'il serait amené à manipuler.
- La confidentialité des mots de passe d'accès aux systèmes et applications.
- La signalisation de toute violation de sécurité ou de confidentialité à l'équipe informatique.
- L'utilisation des informations obtenues uniquement dans un but professionnel.
- La protection des identifiants et Mots de passe en utilisation sur les systèmes d'Information du CHUHII.



4. Confidentialité des données

La préservation des intérêts du CHUHII nécessite le respect par tous d'une obligation générale et permanente de confidentialité, de discrétion et de secret professionnel à l'égard des informations et documents électroniques disponibles au sein du système informatique.

Le respect de cette confidentialité implique notamment de :

- Veiller à ce que les personnes non autorisées n'aient pas connaissance de telles informations ;
- Prendre toutes les mesures nécessaires afin de protéger la confidentialité des données ;
- Veiller à sécuriser tout actif organisationnel (document papier, cd,..) propre au CHUHII.

5. Protection des données à caractère personnel

Une attention particulière est portée au traitement et à la manipulation des données à caractère personnel. A cet effet, il convient de :

- Utiliser les données à caractère personnel pour les strictes finalités pour lesquelles elles sont collectées ;
- Communiquer la destination des informations enregistrées ainsi que leur durée de conservation ;
- Prendre toutes les mesures nécessaires afin de protéger la confidentialité de ces données et assurer leur sécurité et intégrité.

6. Sauvegarde des données

Les données stockées sur le serveur commun sont sauvegardées par le CHUHII et sont sous sa responsabilité. La fréquence de sauvegarde, la durée de rétention et la rotation des supports sont déterminés et affichées au niveau de la politique de sauvegarde.

- Le CHUHII prend en charge la sauvegarde des données des différentes applications installées sur les serveurs de production centralisés dans la salle informatique. En cas de panne ou d'incident, la DSI veillera à remettre le système en état sur la base de la dernière sauvegarde des données avant la panne ;



- Il est impératif à l'utilisateur d'utiliser l'espace disque qui lui est réservé sur le serveur pour le stockage ;
- Le partage de fichiers doit impérativement passer par des plateformes sécurisées approuvées par l'établissement ;
- La DSI décline toute responsabilité en cas de perte globale ou partielle de données ne se trouvant pas sur le serveur. Les postes de travail individuels ne sont pas sauvegardés par la DSI.

7. Usage de la messagerie

L'utilisateur doit faire usage de la messagerie et des services Internet dans le cadre de ses activités professionnelles dans le respect de la législation en vigueur.

En particulier :

- Il est responsable du contenu qu'il insère ou envoie par le biais de la messagerie électronique ;
- Il est interdit de lire ou de prendre connaissance de tout message électronique appartenant ou destiné à une autre personne ;
- Il ne doit pas se connecter ou essayer de se connecter sur un serveur que par les dispositions prévues ;
- Il ne doit pas se livrer à des actions mettant en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède ;
- Il ne doit pas s'approprier l'identité d'une autre personne et il ne doit pas intercepter des communications entre tiers ;
- Il ne doit pas utiliser ces services pour proposer ou rendre accessible aux tiers des données et informations confidentielles ou contraires à la législation en vigueur ;
- Il doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques ;
- Il doit éviter de faire circuler des messages électroniques non professionnels ou portant atteinte à l'intégrité d'un autre utilisateur ou à sa sensibilité, notamment par les messages comportant des images provocantes ou à caractère injurieux, raciste, etc.



10. Gestion des téléphones

- L'utilisation des téléphones fixes et portables fournis par le CHUHII est réservée à des fins professionnelles ;
- L'utilisation des téléphones portables (flotte) à des fins personnelles doit rester occasionnelle et ne doit en aucun cas affecter l'utilisation professionnelle ;
- En cas d'absence, l'utilisateur doit effectuer un renvoi sur le poste d'un autre agent du service ou sur l'accueil téléphonique ;
- L'agent qui quitte définitivement l'établissement doit préalablement restituer le téléphone portable professionnel ;
- L'utilisateur doit veiller à soigner sa présentation lors d'un appel pour faciliter son identification et/ou son service.

11. Gestion des points d'accès

L'utilisation ou l'implémentation des points d'accès non validés par la division informatique du CHUHII est strictement interdite. Cette mesure est mise en place pour renforcer la sécurité de nos systèmes informatiques et pour optimiser la consommation des données au sein de l'organisme.

12. Gestion des accès à distance

L'utilisation des outils et logiciels pour l'accès à distance (TeamViewer, Anydesk...), est strictement interdite au sein du CHUHII. L'accès VPN est donné aux utilisateurs à la suite d'une demande à la direction générale contenant les motifs de cet accès.

13. Analyse et contrôle de l'utilisation du système informatique

Pour des nécessités de maintenance et de gestion technique, l'utilisation des équipements informatiques ou logiciels ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect de la confidentialité du traitement.

Le CHUHII se réserve notamment le droit de :

- Vérifier le trafic informatique entrant et sortant ainsi que le trafic transitant sur le réseau interne ;



- Faire des audits pour vérifier que les consignes d'usage et les règles de sécurité sont appliquées ;
- Contrôler les logiciels installés ;
- Filtrer les adresses électroniques (URL) des sites non autorisés ;
- Tracer et auditer tous les accès aux services Intranet et Internet.

14. Utilisation Internet

L'accès internet mis à la disposition des utilisateurs par l'établissement est uniquement pour une utilisation professionnelle, plus spécifiquement pour des tâches reliées à l'exercice des fonctions de ses utilisateurs. A cet effet, l'utilisateur ne doit pas :

- Profiter des facilités d'accès à Internet pour propager un virus sur les réseaux informatiques de l'établissement ;
- Profiter des facilités d'accès à Internet pour importer ou télécharger ou installer les proxy sur les réseaux informatiques de l'établissement ;
- Se servir des facilités d'accès à Internet ou au réseau intégré de télécommunication multimédia ou à tout autre moyen pour rendre inutilisable ou surcharger les ordinateurs et le réseau (exemple : Social media, streaming...);
- Violer les droits d'accès à l'internet données par la division informatique selon le besoin ;
- Utiliser des connexions internet autres que celle offerte par le CHUHII pour connecter les équipements de l'établissement.

15. Activités interdites

Tout utilisateur s'interdit de consulter, charger, stocker, publier ou diffuser via les moyens informatiques et de communication SI, des documents, informations, programmes, images, fichiers, ..., contraire à la loi ou à l'ordre public et plus particulièrement :

- De caractère diffamatoire et de manière générale illicite ;
- Portant atteinte aux ressources du CHUHII et plus particulièrement à l'intégrité et à la conservation des données du CHUHII ;
- Portant atteinte à la confidentialité des informations et données du CHUHII et/ou de ses utilisateurs ;



- Portant atteinte à l'image interne et externe du CHUHII ;
- Relatifs à la vie privée d'une personne ou à son image, sans avoir reçu son autorisation formelle d'utiliser l'information ou l'image en question ;
- Protégés par les lois sur la propriété intellectuelle, autres que ceux qui sont mis à sa disposition et expressément autorisés par le CHUHII.
- Ainsi, il est formellement interdit :
 - D'utiliser des programmes qui saturent les ressources ou inondent la bande passante ;
 - D'introduire des programmes nuisibles (cheval de Troie, virus, ou autres) ;
 - D'effectuer des actes de piratage ou d'espionnage ;
 - Tracer et auditer tous les accès aux services Intranet et Internet.

16. Révision de la charte

La présente charte a été rédigée dans l'intérêt de chacun des utilisateurs. Elle sera régulièrement mise à jour, par le Responsable de la Sécurité des Systèmes d'Information, pour tenir compte de l'évolution constante de l'environnement et des techniques informatiques.

La charte d'utilisation des ressources informatiques du CHUHII devra être revue et enrichie en cas de :

- Changements majeurs dans le système d'information et les ressources informatiques du CHUHII ;
- Détection d'incidents fréquemment rencontrés par les utilisateurs.

17. Entrée en vigueur

La présente Charte entrera en application dès sa signature.

Fès le 10 Juin 2024

