Synthèse de la Charte d'Utilisation du Système d'Information du Centre Hospitalier de Dunkerque

La charte d'utilisation du Système d'Information s'inscrit dans le cadre de la politique de sécurité du Système d'Information du Centre Hospitalier de Dunkerque, ci-après nommé « établissement ».
Celle-ci présente **les droits et devoirs** liés à l'utilisation des ressources informatiques au sein de l'établissement et est consultable sur le portail Intranet dans la rubrique Informatique / Documents de références.
Ce document présente un résumé de chacun des points qui y sont abordés.

Les droits et devoirs de l'utilisateur

Un utilisateur est une personne physique autorisée à accéder au système d'information de l'établissement. Chaque utilisateur est **responsable** de la protection des données de par l'usage qu'il fait du système d'information.

Accès aux ressources : Toute personne travaillant, à titre permanent ou temporaire, au sein de l'établissement dispose d'un droit d'accès au système d'information, au regard de ses besoins. Ce droit d'accès doit être **strictement personnel, unique, réservé et justifié.**

Authentification : Ce droit d'accès est strictement personnel. Il ne doit être ni communiqué, ni prêté ni cédé à un tiers. La direction Informatique doit être obligatoirement contactée pour tout problème lié à cet identifiant (perte de mot de passe, oubli, difficultés de connexion, usurpation d'identité).

Déconnexion : Toute personne doit veiller à se déconnecter des applications du SIH lorsqu'elle quitte son travail, et veiller à ce que ses identifiants ne soient pas utilisés pendant son absence.

Respect de la confidentialité : l'utilisateur est tenu au secret professionnel concernant les données auxquelles il accède. Il doit donc veiller à la discrétion et la non diffusion de ces données.

Déclaration des données nominatives : si l'utilisateur est amené à constituer des fichiers nominatifs, il se doit légalement de déclarer ceux-ci à la CNIL.

Protection des données : toutes les données des applications du SIH et toutes les données hébergées sur les serveurs accessibles sur le réseau sont sécurisées et sauvegardées. Par contre, toutes les données locales (présentes sur les disques durs des PC) ne sont ni sauvegardées, ni protégées. Il est alors à la charge de l'utilisateur de veiller à leur non divulgation et à leur sauvegarde si nécessaire.

Utilisation du matériel de l'établissement : le matériel mis à disposition par l'établissement est un outil de travail. Nul ne peut prétendre à un droit de propriété particulier. Tout matériel non fourni par l'établissement ne peut être connecté au réseau.

Protection des supports physiques : Les supports amovibles (CD, DVD, clés USB…) sont sous la responsabilité de l'utilisateur. Les données nominatives s'y trouvant stockées doivent être chiffrées.

Utilisation des logiciels : Seuls les logiciels sous licence valide et approuvés par la Direction Informatique peuvent être installés sur les matériels de l'établissement.

Utilisation de la messagerie : Le message électronique est un écrit qui engage la responsabilité de son auteur et éventuellement celle de l'établissement. Il peut être reconnu pour établir un fait ou un acte juridique. L'usage doit en être fait dans une attitude de bon sens, en respectant les règles de chiffrement pour les envois de données nominatives.
La liste des destinataires doit être appropriée à l'objet du mail.

Centre Hospitalier de Dunkerque – 130 Avenue Louis Herbeaux - CS 76.367 – 59385 DUNKERQUE CEDEX 1
dam@ch-dunkerque.fr

Utilisation d'Internet : L'utilisateur s'engage à n'utiliser Internet qu'à des fins strictement professionnelles.
Il est informé de la mise en place d'une trace des accès qui peut être exploitée en cas de nécessité. Un filtrage des sites pouvant mettre en jeu la responsabilité de l'établissement (sites à caractère violent, pornographique, extrémiste politique ou religieux ou de piratage informatique) est également mis en place.

Utilisation de la téléphonie : Des téléphones peuvent être mis à disposition des utilisateurs. Leur utilisation est strictement réservée à des fins professionnelles.

Intégrité des systèmes : L'utilisateur doit veiller à préserver l'intégrité des systèmes mis à sa disposition. L'utilisation anormale du matériel, l'introduction de logiciels et de matériels non validés par le Service Informatique et le contournement des règles de sécurité mises en place sont strictement interdits.

Protection antivirale : La désactivation des logiciels anti-virus est interdite, sauf sur avis express de la direction informatique. L'introduction volontaire, la propagation ou l'exécution de codes malveillants au sein des systèmes d'information de l'établissement sont strictement interdits, y compris à des fins de tests.

Incidents de sécurité : Tout événement remettant en cause la sécurité du système d'information de l'établissement doit être immédiatement signalé par l'utilisateur auprès de la direction informatique. L'utilisateur ne doit en aucun cas essayer de réparer lui-même les dysfonctionnements observés ou alors tenter de prouver l'existence d'une faille de sécurité.

Les droits et les devoirs de l'établissement

Intégrité des systèmes : L'établissement met en place des dispositifs et règles de sécurité sur les postes de travail, réseaux et systèmes garantissant le niveau d'intégrité du système d'information, en particulier pour les données médicales.

Protection antivirale : L'établissement met en place des dispositifs de sécurité pour protéger son système d'information contre toute attaque virale provenant de l'interne ou de l'extérieur.

Respect de la topologie du réseau : L'établissement prend toutes dispositions techniques pour protéger son réseau et son SIH des intrusions ou malveillances externes.

Cryptographie des données sensibles : Les informations sensibles transmises via les réseaux publics sont obligatoirement chiffrées.

Surveillance dans l'établissement : L'utilisation abusive des équipements informatiques peut engager la responsabilité de l'établissement. Il lui appartient donc de prendre les dispositions nécessaires au contrôle du respect des règles.
L'établissement peut donc mettre en place, dans le respect de la législation en matière de confidentialité et de vie privée des utilisateurs, les dispositifs de traçabilité et de contrôle définis dans le document « politique de traçabilité de l'établissement».

Tentatives de violation des procédures de sécurité : Le contournement, ou la simple tentative de contournement des dispositifs de sécurité mis en place par l'établissement est strictement interdit.

Sanctions et poursuites : L'établissement est responsable du SIH, des outils informatiques et de l'usage qui en est fait. Cependant en cas de violation manifeste des règles énumérées dans ce document, et/ou des règlements, des lois et des usages en vigueur, l'utilisateur engage sa propre responsabilité et l'établissement est en droit d'engager des éventuelles poursuites à l'encontre des contrevenants.

Je soussigné(e) ....., membre du Centre Hospitalier de Dunkerque, déclare avoir pris connaissance de la charte d'utilisation du Système d'Information du CHD, et m'engage à m'y conformer strictement.

Fait à Dunkerque le .. / .. / 20..

Centre Hospitalier de Dunkerque – 130 Avenue Louis Herbeaux - CS 76.367 – 59385 DUNKERQUE CEDEX 1
dam@ch-dunkerque.fr