



CENTRE HOSPITALIER VALVERT

Charte informatique

La présente charte a pour objet de définir les règles d'utilisation des moyens informatiques mis à la disposition du personnel du centre hospitalier Valvert et ainsi :

- Assurer la sécurité du système d'information
- Préserver la confidentialité des données
- Maintenir les performances du système
- Limiter la prolifération erratique des logiciels
- Eviter l'atteinte à des droits privatifs

Définitions

On appelle "Utilisateur" toute personne, quel que soit son statut, ayant accès ou utilisant les ressources informatiques dans le cadre de son emploi au sein de l'établissement.

Par « ressources informatiques », on entend :

- les moyens informatiques matériels : serveurs, ordinateurs, imprimantes, et tout autre équipement informatique.
- les logiciels, qu'ils soient sur l'ordinateur de l'utilisateur ou accessibles à distance sur le serveur de l'établissement (Intranet) ou autres serveurs externes (Internet).

1. Domaine d'application de la charte

Les règles décrites dans la présente charte s'appliquent à tout le personnel du centre hospitalier Valvert qui utilise les moyens informatiques de l'hôpital, ainsi que tout autre moyen de connexion à distance afin d'accéder, via le réseau informatique de Valvert, à tout service de communication ou de traitement électronique interne ou externe, y compris l'accès sur l'Internet et ce, directement ou en cascade.

Le non-respect d'une de ces règles est susceptible d'entraîner des mesures disciplinaires internes voire, en cas de violation d'un texte législatif ou réglementaire, des poursuites judiciaires. Les diverses lois concernées par ce document sont présumées connues, en particulier la loi Informatique et Liberté 92-684 du 22/07/1992, la loi relative à la fraude informatique 92-685 du 22/07/1992, le code de la propriété intellectuelle 92-597 du 01/07/1992, la loi relative aux infractions de presse du 29/07/1881, modifiée, sanctionnant notamment la diffamation, le



CENTRE HOSPITALIER VALVERT

négationnisme, le racisme et les injures et la loi relative aux infractions aux règles de cryptologie du 29/12/1990 modifiée le 26/07/1996.

2. Conditions d'accès de l'utilisateur

L'utilisation des ressources informatiques du centre hospitalier Valvert est soumise à autorisation préalable :

1. Cette autorisation est concrétisée par l'ouverture d'un compte et par l'utilisation d'un poste de travail.
2. Cette autorisation est strictement personnelle et ne doit en aucun cas être cédée, même temporairement, à un tiers.
3. Cette autorisation ne vaut que pour les activités conformes aux missions du centre hospitalier Valvert, dans le respect de la législation en vigueur rappelée ci-dessus et que pour les missions confiées à l'agent.
4. Le centre hospitalier Valvert se réserve le droit de retirer à tout moment cette autorisation et ce, sans préavis.
5. Chaque utilisateur doit user raisonnablement des ressources partagées auxquelles il accède. L'usage de ces ressources est par ailleurs limité à des utilisations professionnelles.

3. Respect de la confidentialité des informations

1. Les utilisateurs ne doivent pas tenter de lire, de copier, de divulguer ou de modifier les fichiers d'un autre utilisateur sans y avoir été autorisés.
2. Les utilisateurs doivent s'interdire toute tentative d'interception de communications entre tiers.
3. Les utilisateurs sont tenus à la réserve d'usage sur toute information relative au fonctionnement interne du centre hospitalier Valvert qu'ils auraient pu obtenir en utilisant ces ressources informatiques.
4. Les utilisateurs sont tenus de prendre, avec l'aide éventuelle de la DSIO, les mesures de protection des données nécessaires au respect des engagements de confidentialité pris par le centre hospitalier Valvert vis-à-vis de tiers.



CENTRE HOSPITALIER VALVERT

4. Règles de sécurité

Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques du centre hospitalier Valvert à partir des comptes qui lui ont été ouverts ou des matériels mis à sa disposition. Il doit donc, en ce qui le concerne et à l'aide des recommandations fournies par la DSIO, contribuer à la sécurité du système d'information.

En particulier :

1. Tout utilisateur doit choisir des mots de passe sûrs respectant les recommandations de la DSIO. Ces mots de passe doivent être gardés secrets, modifiés régulièrement et en aucun cas être communiqués à qui que ce soit.
2. Tout utilisateur est responsable des ressources auxquelles il a accès.
3. Les utilisateurs ne doivent pas utiliser des comptes autres que ceux pour lesquels ils ont reçu une autorisation. Ils doivent s'abstenir de toute tentative de s'approprier ou de déchiffrer le mot de passe d'un autre utilisateur.
4. L'utilisation et le développement de programmes mettant sciemment, ou risquant de mettre en cause l'intégrité des systèmes informatiques, sont interdits.
5. Sur les sites, tout utilisateur doit respecter les modalités de raccordement des matériels aux réseaux de communication internes et externes, telles qu'elles sont fixées par la DSIO. Ces raccordements ne peuvent être modifiés qu'avec son autorisation préalable. Ces modalités couvrent à la fois des aspects matériels (connexion physique) et logiciel (connexion logique).
6. Tout constat de violation, tentative de violation ou soupçon de violation d'un système informatique doit être signalé à l'un des membres de la DSIO.
7. Les utilisateurs sont tenus de respecter les consignes de la DSIO.

5. Obligations relatives à la propriété des logiciels et des œuvres protégées par le droit d'auteur

L'utilisation des logiciels et plus généralement de tout document (fichier, image, son) doit se faire dans le respect de la propriété intellectuelle (loi 92-597 du 1er juillet 1992), des recommandations fixées par les détenteurs de droits et des engagements pris par le centre hospitalier Valvert (dans les contrats de licences par exemple). En particulier :



CENTRE HOSPITALIER VALVERT

1. La reproduction de logiciel est interdite. Seul l'établissement d'une copie de sauvegarde pourra être autorisé par DSIO.
2. Il est strictement interdit d'installer sur un système du centre hospitalier Valvert un logiciel quelconque, sans en avoir fait la demande auprès de la DSIO.

6. Obligations relatives aux données nominatives

Toute constitution, à l'aide des moyens informatiques de l'hôpital ou sur son réseau de traitements de données nominatives doit faire l'objet, préalablement à leur mise en œuvre, d'une déclaration ou d'une demande d'avis auprès de la Commission nationale informatique et libertés.(loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés).

Toute personne utilisant des moyens informatiques mis à sa disposition par le Centre hospitalier Valvert s'engage à demander l'autorisation de la DSIO pour posséder ou créer de tels fichiers. Le directeur du Centre hospitalier Valvert effectuera auprès de la CNIL les démarches nécessaires.

7. Accès aux ressources informatiques et services Internet

L'utilisation des ressources informatiques et l'usage des services Internet ainsi que ceux du réseau pour y accéder ne sont autorisés que dans le cadre exclusif de l'activité professionnelle des utilisateurs conformément à la législation en vigueur.

Il est rappelé à ce titre, que la navigation sur des sites et ou la sauvegarde de documents à caractère raciste, pédophile...est punissable par la loi n°227-23 du code pénal.

L'utilisation des ressources informatiques partagées et la connexion d'un équipement sur le réseau sont en outre soumises à autorisation. Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Ces autorisations peuvent être suspendues à tout moment. Toute autorisation prend fin lors de la cessation même provisoire de l'activité professionnelle qui l'a justifiée.

L'hôpital pourra en outre prévoir des contrôles et des restrictions d'accès spécifiques à son organisation : (Authentification, filtrage des sites accessibles, taille des fichiers joints...)

Tout utilisateur est responsable de l'usage des ressources informatiques et du réseau auxquels il a accès. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale de l'hôpital.

Ne sont, notamment, pas autorisés les pratiques suivantes :

- le téléchargement de vidéo, d'images animées, de banques de son non liées à l'activité professionnelle de l'utilisateur



CENTRE HOSPITALIER VALVERT

- la diffusion de tracts par messagerie
- le « *spam* » (diffusion d'un document en grand nombre)
- les forums ne sont autorisés que dans le cadre de groupes de travail reconnus par l'Institution
- le principe de « chaîne » c'est-à-dire la diffusion collective démultipliée par le biais du receveur d'information.

L'utilisateur doit faire usage des services Internet dans le cadre exclusif de ses activités professionnelles dans le respect de la législation en vigueur. Seuls ont vocation à être consultés les sites Internet présentant un lien direct et nécessaire avec l'activité professionnelle, sous réserve que la durée de connexion n'excède pas un délai raisonnable et présente une utilité au regard des fonctions exercées

La DSIO pourra mettre en œuvre des moyens permettant :

- le filtrage de sites Internet non autorisés (à caractère pornographique, xénophobe, ...).
- l'interdiction de télécharger des logiciels.
- le contrôle à posteriori des données de connexion à Internet.
- l'élaboration de fichiers de journalisation des connexions afin de garantir une utilisation normale des ressources.
- la « prise de mains à distance » pour détecter et réparer les pannes à distance du poste de travail.

Les messages électroniques sont assimilés à des messages privés et ont donc un caractère confidentiel.

Le contenu des informations véhiculées, par quelque moyen que ce soit, à l'intérieur ou à l'extérieur de l'établissement, est sous l'entière responsabilité personnelle de l'émetteur; en aucun cas l'établissement ou la direction ne sauraient être tenus pour responsables d'une utilisation malveillante ou frauduleuse qui aurait causé des préjudices à des tiers.



CENTRE HOSPITALIER VALVERT

Rappel des principales lois

- la loi du 6/1/78 dite informatique et liberté ;
- la législation relative à la fraude informatique (article 323-1 à 323-7 du Code pénal);
- la loi du 10/07/91 relative au secret des correspondances émises par voie de télécommunication ;
- la législation relative à la propriété intellectuelle ;
- la loi du 04/08/1994 relative à l'emploi de la langue française ;
- la législation applicable en matière de cryptologie, notamment l'article 28 de la loi du 29/12/90 sur la réglementation des télécommunications dans sa rédaction issue de l'article 17 de la loi du 26/07/96 et par ses décrets d'application du 24/02/98, 23/03/98 et 17/03/99;
- la directive 96/9CE du 11 mars 1996 concernant la protection juridique des bases de données ;
- la loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé ;
- loi n°227-23 du code pénal, qui criminalise le fait, de fixer, d'enregistrer ou de transmettre, en vue de sa diffusion, l'image ou la représentation d'un mineur qui présente un caractère pornographique.



CENTRE HOSPITALIER VALVERT

ANNEXE

Quelques règles de bon usage :

- Attention à ne pas divulguer, par quelque moyen que ce soit (téléphone, Fax, Internet, ...) une information à caractère confidentiel.
- L'utilisateur doit protéger ses données d'une éventuelle intrusion ; il est responsable des droits qu'il donne aux autres utilisateurs.
- Le contenu des informations véhiculées à l'intérieur et à l'extérieur de l'établissement est sous l'entière responsabilité personnelle de l'émetteur.
- L'utilisateur devra être prudent lors de sollicitations extérieures et veiller à toujours demander l'avis du directeur lors de la réalisation de données statistiques, que ces données soient médicales ou non.
- Le droit d'accès à un système informatique est personnel et incessible. A chaque utilisateur relié au réseau informatique interne de l'établissement est associé un compte utilisateur, un mot de passe personnel, ainsi qu'une adresse de messagerie électronique.
- Les fichiers individuels ou collectifs sont privés, même s'ils sont physiquement accessibles : la possibilité matérielle de lire un fichier n'implique pas l'autorisation de le lire !
- Il appartient à chaque agent de divulguer lui-même son adresse électronique professionnelle, il n'est pas du ressort des agents du standard (ou des secrétaires) de le faire, sauf accord de son propriétaire.
- La saisie du nom d'utilisateur permet l'identification ; la saisie du mot de passe permet l'authentification.
- Il convient à chaque utilisateur de modifier ses mots de passe régulièrement, au moins chaque trimestre, et de les garder secrets.
- L'utilisateur doit être vigilant par rapport aux personnes utilisant son poste de travail ; (par exemple, un fournisseur doit impérativement être accompagné pour assurer toute intervention).
- Il doit signaler toute tentative de violation de son compte et toute anomalie.
- Il ne doit pas mettre à la disposition d'utilisateurs non autorisés un accès au système ou aux réseaux, à travers des matériels dont il a l'usage.
- Il ne doit pas utiliser des comptes autres que le sien.
- Il ne doit pas tenter, directement ou indirectement, de lire, modifier, copier ou détruire des données autres que celles qui lui appartiennent en propre.
- Il ne doit pas quitter son poste de travail sans se déconnecter en laissant des ressources ou services accessibles.
- Si, dans son travail, l'utilisateur est conduit à constituer des fichiers tombant sous le coup de la loi Informatique et Libertés, il devra auparavant en avoir fait la demande à la DSIO qui en fera la déclaration auprès de la CNIL.