



 CENTRE HOSPITALIER  
UNIVERSITAIRE DE QUÉBEC

## *Politique en matière de sécurité informationnelle*

**CENTRE HOSPITALIER UNIVERSITAIRE DE QUÉBEC**

**Ce document est réservé à l'usage exclusif des membres du conseil d'administration**

**Janvier 2004**

Janvier 2004

Version 3.0

© Tous droits réservés. Centre hospitalier universitaire de Québec, 2003-2004. Toute reproduction interdite.

***Documents source***

«Politique relative à la sécurité des actifs informationnels et de télécommunications et à la protection des données et des renseignements confidentiels», Centre hospitalier universitaire de Québec, 1999-2001.

«Cadre global de gestion des actifs informationnels appartenant aux organismes du réseau de la Santé et des Services sociaux – volet sur la sécurité», ministère de la Santé et des Services sociaux, 24 septembre 2002.

***Préparé par :***

Yvan Fournier – *officier de sécurité informationnelle*  
Centre hospitalier universitaire de Québec

Louise Côté– *assistante à l'officier de sécurité informationnelle*  
Centre hospitalier universitaire de Québec

Novembre 2003

## Table des matières

PRÉAMBULE .....	1
1. INTRODUCTION .....	1
2. OBJECTIFS DE LA POLITIQUE .....	2
3. DOMAINE D'APPLICATION .....	3
4. PRINCIPES DIRECTEURS .....	3
4.1. CUEILLETTE DE RENSEIGNEMENTS NOMINATIFS .....	3
4.2. CONFIDENTIALITÉ DES RENSEIGNEMENTS NOMINATIFS ET LEUR COMMUNICATION .....	4
4.3. ACCÈS AUX ACTIFS INFORMATIONNELS ET DE TÉLÉCOMMUNICATIONS .....	4
4.4. UTILISATION D'INTERNET .....	4
4.5. UTILISATION DU RÉSEAU DE TÉLÉCOMMUNICATION SOCIO SANITAIRE (RTSS <sup>MO</sup> ) ET DES RÉSEAUX D'INFORMATIONS DU CHUQ .....	5
4.6. COURRIER ÉLECTRONIQUE .....	5
5. ÉNONCÉ DE LA POLITIQUE : .....	5
MESURES DE CONTRÔLE .....	5
5.1. ORGANISATION DE LA SÉCURITÉ .....	5
5.2. ACCÈS AUX RENSEIGNEMENTS NOMINATIFS, PERSONNELS OU CONFIDENTIELS .....	5
5.3. UTILISATION D'INTERNET, D'INTRANET ET DES RÉSEAUX D'INFORMATIONS DU CHUQ .....	6
5.4. UTILISATION DU COURRIER ÉLECTRONIQUE .....	8
5.5. UTILISATION DU TÉLÉTRAVAIL .....	9
5.6. UTILISATION DES TECHNOLOGIES SANS FILS .....	9
5.7. COPIES DE SÉCURITÉ .....	9
5.8. COPIES DE SOURCE EXTERNE .....	9
5.9. DÉVELOPPEMENT ET CONCEPTION D'APPLICATIONS ET PROJETS D'INFORMATISATION .....	9
5.10. GESTIONS DES DOCUMENTS .....	9
5.11. UTILISATION DES IMPRIMANTES ET DES TÉLÉCOPIEURS .....	9
5.12. SÉCURITÉ DES TÉLÉCOMMUNICATIONS .....	10
5.13. MESURES DE SÉCURITÉ .....	10
5.14. ÉVALUATION DE LA SÉCURITÉ .....	11
5.15. PROGRAMME D'INFORMATION, DE SENSIBILISATION ET DE FORMATION DU PERSONNEL .....	11
5.16. MANQUEMENTS À LA SÉCURITÉ .....	11
5.17. MISE À JOUR DE LA POLITIQUE .....	11
5.18. RÔLES ET RESPONSABILITÉS DU CHUQ : .....	12
5.18.1. <i>Le conseil d'administration</i> .....	12
5.18.2. <i>Le directeur général</i> .....	12
5.18.3. <i>L'officier de sécurité informationnelle</i> .....	12
5.18.4. <i>Le gestionnaire du personnel utilisateur</i> .....	14
5.18.5. <i>Le comité de sécurité informationnelle</i> .....	14
5.18.6. <i>Le responsable de l'application de la Loi sur l'accès aux documents des organismes                 publics et sur la protection des renseignements personnels</i> .....	14
5.18.7. <i>Les utilisateurs</i> .....	14
5.19. ENGAGEMENT DE CONFIDENTIALITÉ PAR LES TIERS OU LE PERSONNEL DES FOURNISSEURS DE SERVICES DU CHUQ .....	16
6. MISE EN APPLICATION .....	15

ANNEXES

ANNEXE I - ENGAGEMENT DE CONFIDENTIALITÉ TYPE .....	17
ANNEXE II - DÉCLARATION DE L'EMPLOYÉ QUANT À LA CONNAISSANCE ET AU RESPECT DE LA POLITIQUE EN MATIÈRE DE SÉCURITÉ INFORMAIONNELLE .....	19
ANNEXE III - CODE DE CONDUITE DES UTILISATEURS .....	19
ANNEXE IV - CODE DE CONDUITE DES INFORMATIENS ET ADMINISTRATEURS DE RÉSEAUX D'INFORMATIONS .....	23
ANNEXE V - CODE DE CONDUITE DU PERSONNEL DES FOURNISSEURS DE SERVICES OU D'UN TIERS .....	25
ANNEXE VI - CODE DE CONDUITE DES UTILISATEURS D'ORDINATEURS PORTATIFS.....	26
ANNEXE VII- CODE DE CONDUITE DES UTILISATEURS D'INTERNET.....	29
RÉFÉRENCES .....	32
DÉFINITIONS .....	33

## Préambule :

Issu de la fusion en décembre 1995 de trois hôpitaux, CHUL, Hôpital St-François d'Assise et L'Hôtel-Dieu de Québec, le Centre hospitalier universitaire de Québec (ci-après désigné CHUQ) est un établissement à vocation suprarégionale ayant pour mission d'offrir des soins généraux et ultraspécialisés à la clientèle de la région de Québec et de tout l'est du Québec.

En sa qualité d'hôpital universitaire de soins, d'enseignement et de recherche, et en vertu d'ententes avec l'Université Laval, le CHUQ collabore à des activités d'enseignement et de recherche, procède à l'évaluation des technologies et participe à des activités de promotion de la santé.

Dans ce contexte qui favorise l'émergence des connaissances, le CHUQ s'applique à développer des approches novatrices afin d'améliorer la santé de la population.

## 1. Introduction

L'intégration de plus en plus grande des systèmes d'informations à la majorité des activités du CHUQ, regroupant les activités de soutien administratif et médico-hospitalier, favorisent l'accessibilité à toutes sortes de renseignements par les intervenants du CHUQ, incluant les fournisseurs de services et les tiers. Par conséquent, afin d'éviter toute divulgation de documents confidentiels et assurer la sécurité en regard de l'utilisation des systèmes d'informations, une *Politique relative à la sécurité des actifs informationnels et de télécommunications et à la protection des données et des renseignements confidentiels* a été adoptée par le conseil d'administration du CHUQ le 9 février 2000 et mise en application.

Plus spécifiquement, cette politique a été établie dans le but de mettre en place des mesures et des mécanismes administratifs et de contrôle afin d'assurer le respect des droits des usagers, tel que stipulé dans la « *Loi des services de santé et des services sociaux* », la « *Loi sur les archives* » la « *Charte des droits et libertés de la personne* », la « *Loi sur l'accès aux des organismes publics et sur la protection des renseignements personnels* ». De plus en 2002, le MSSS approuvait le *Cadre global de gestion des actifs informationnels appartenant aux organismes du réseau de la santé et des services sociaux – Volet sur la sécurité* (ci-après désigné Cadre global) du MSSS lequel document précise les orientations et obligations que doivent rencontrer les organismes du réseau de la santé et des services sociaux en matière de sécurité de l'information.

Dans cette optique, le CHUQ doit mettre en place un ensemble de mesures de sécurité et de contrôle afin de protéger les renseignements confidentiels et les données sociosanitaires nominatives informatisées, de gérer adéquatement l'utilisation d'Internet, du courrier électronique et des réseaux d'information du CHUQ tant au niveau des travaux de recherche scientifique, de l'enseignement, du domaine médico-administratif ou de toute autre mandat qui pourrait lui être confié. Ceci ne restreint pas la mise en place de mesures de sécurité supplémentaires ou plus restrictives afin de s'assurer de la protection des documents confidentiels qui sont confiés à chaque organisme ou établissement du CHUQ ou en faisant partie.

Ce document présente donc les objectifs de la présente politique, le domaine d'application, les principes directeurs et l'énoncé de celle-ci.

Cette politique a été adoptée par le conseil d'administration du CHUQ le 9 février 2000 et est entrée en vigueur à cette date. Le présent document constitue une mise à jour de ladite politique qui portera dorénavant le titre suivant : ***Politique en matière de sécurité informationnelle*** (ci-après désignée Politique).

La forme électronique du texte intégral de la politique est disponible sur le site web du CHUQ à l'adresse suivante : [www.chuq.qc.ca](http://www.chuq.qc.ca) sous l'onglet : Politiques, sur l'intranet, sous la rubrique DFSIG, sécurité informatique, politique, présenté sous sa forme intégrale et résumée, ainsi que dans le dépôt de documents de Lotus Notes<sup>MC</sup>.

## 2. Objectifs de la politique

La présente politique a pour objectifs d'assurer:

- la disponibilité, l'intégrité et la confidentialité des documents traités par les réseaux d'informations du CHUQ;
- que les renseignements confidentiels relatifs aux usagers et au personnel du CHUQ soient protégés par des mesures de contrôle des accès autorisés dans l'exercice des fonctions de chaque personne;
- la sécurité en regard de l'utilisation des réseaux d'informations du CHUQ, des actifs informationnels et de télécommunications, du matériel informatique et des données nominatives, corporatives ou institutionnelles;
- le respect des différents Codes de conduite concernant l'utilisation et la gestion des technologies de l'information et des télécommunications adoptés par le CHUQ.

Ce cadre réglementaire et les règles qui y sont associées visent à assurer le respect du cadre légal à l'égard de l'usage et du traitement de l'information, plus particulièrement des données sociosanitaires confidentielles, des données relatives à la propriété intellectuelle, ou des renseignements de toute nature concernant une recherche, lesquelles sont qualifiés de strictement confidentiels, ainsi que de l'utilisation des actifs informationnels et de télécommunications.

La présente politique couvre:

- tous les actifs informationnels et de télécommunications appartenant ou sous la responsabilité du CHUQ;
- les contrats ou les ententes de services avec tout intervenant externe. Les ententes doivent contenir les dispositions requises pour garantir le respect de la présente politique et les règles qui en découlent.

Cette politique couvre, de même, tous les documents traités par le CHUQ dans le cadre de ses fonctions et de ses mandats. Ceci englobe tout le matériel informatique qui conserve, transmet et traite des données informatiques, quel que soit le type de support utilisé: bandes magnétiques, disquettes, CD-ROM, listes ou toute autre forme. Également, ceci concerne toute la gestion et la disposition des documents et des informations qu'ils contiennent.

### 3. Domaine d'application

La présente politique s'applique à tous les utilisateurs de systèmes d'informations qui, de près ou de loin, peuvent avoir accès aux actifs informationnels et de télécommunications ainsi qu'aux documents qu'ils supportent.

Elle s'étend aux tiers, c'est-à-dire à toute personne physique ou morale qui utilise ou accède au nom du CHUQ, ou non, à des informations confidentielles ou non, quel que soit le support sur lesquelles elles sont portées. Cette tierce partie peut être désignée comme fournisseur de services ou tiers dans la présente politique.

Certains membres du personnel, par la teneur de leurs fonctions peuvent être amenés à être en contact avec de tels documents. Citons à titre d'exemple le personnel de l'entretien ménager, des services techniques ou des sous-traitants.

### 4. Principes directeurs

Les principes directeurs émis dans cette politique sont tirés du *Cadre global de gestion des actifs informationnels appartenant aux organismes du réseau de la santé et des services sociaux – Volet sécurité*, approuvé par le MSSS le 24 septembre 2002. Ces principes s'articulent autour de la cueillette, de la confidentialité des renseignements nominatifs et leur communication, de l'accès aux données confidentielles, aux actifs informationnels et de télécommunications et à l'ensemble des activités concernant l'acquisition, la production, le traitement, l'entreposage, le transfert et l'impression ainsi que la disposition des informations.

#### 4.1. Cueillette de renseignements nominatifs

La «Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels» prescrit, à l'article 64, les règles relatives à la cueillette de renseignements personnels :

*64. Nul ne peut, au nom d'un organisme public, recueillir un renseignement nominatif si cela n'est pas nécessaire à l'exercice des attributions de cet organisme ou à la mise en œuvre d'un programme dont il a gestion.*

Il est donc interdit de recueillir un renseignement personnel si cela n'est pas requis.

#### **4.2. Confidentialité des renseignements nominatifs et leur communication**

Le dossier des usagers est soumis à la plus stricte confidentialité tel que mentionné dans les différentes lois. À titre d'exemples l'article 53 de la « *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* » et l'article 19 de la « *Loi sur les services de santé et les services sociaux* » stipulent qu'aucun renseignement ne peut être tiré du dossier sans le consentement de l'individu concerné.

La Commission d'accès à l'information du Québec privilégie pour sa part un consentement libre, éclairé et donné par écrit par la personne concernée. Nous rappelons par ailleurs que souvent, les informations demandées ne concernent pas toujours l'ensemble du dossier de la personne.

Ce même article 19 de la « *Loi sur les services de santé et les services sociaux* » prévoit des exceptions au principe du consentement. Dans ces cas bien particuliers - et exceptionnels -, les informations peuvent être transférées en autant que leur confidentialité soit garantie. De plus, pour des secteurs d'activités spécifiques, le législateur dégage l'organisme de l'obligation d'obtenir un consentement de l'utilisateur selon des conditions spécifiées par celui-ci. Par exemple, pour ne citer que ce cas, le législateur prévoit que le directeur de la Santé publique n'a pas à obtenir le consentement de l'utilisateur en ce qui concerne les maladies à déclaration obligatoire.

Aucun renseignement ne peut donc être retiré du dossier d'un usager sans le consentement de celui-ci, sauf exceptions prévues par la loi.

#### **4.3. Accès aux actifs informationnels et de télécommunications**

L'accès aux actifs informationnels et de télécommunications du CHUQ par le personnel, ou des tiers, doit être contrôlé. Chaque système prévoit des privilèges d'accès différents selon les catégories de personnel.

Le CHUQ limite l'accès de leurs actifs informationnels et de télécommunications aux seules personnes dont les tâches l'exigent dans l'exercice normal de leurs fonctions et qui détiennent en conséquence un privilège d'accès approprié.

#### **4.4. Utilisation d'Internet**

Internet est un outil mis à la disposition du personnel du CHUQ pour une utilisation professionnelle, plus spécifiquement pour des tâches reliées à l'exercice des fonctions de celui-ci.

À cet effet, la présente politique émet des mesures dans le but que chacun utilise cet accès avec vigilance, en respectant les droits d'auteur, la propriété intellectuelle, les règles de licences de logiciels, les droits de propriété, la confidentialité des informations et des données, en faisant bon emploi des ressources et des outils disponibles et en respectant les lois et règlements émis par le Législateur.

#### **4.5. Utilisation du réseau de télécommunications sociosanitaires (RTSS<sup>MO</sup>) et des réseaux d'informations du CHUQ**

Le personnel du CHUQ a accès à un réseau intranet, au RTSS<sup>MO</sup> et aux réseaux d'informations mis en place par le CHUQ. Ceux-ci doivent être utilisés uniquement pour des raisons professionnelles.

La présente politique présente des mesures de sécurité qui sont associées à l'utilisation desdits réseaux par les utilisateurs pour assurer la disponibilité, l'intégrité, la confidentialité de l'information, ainsi que l'irrévocabilité des actes posés par les utilisateurs.

#### **4.6. Courrier électronique**

Les messages et fichiers électroniques circulant au CHUQ sont soumis aux dispositions de la « *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* » et de la « *Loi sur la protection des renseignements personnels dans le secteur privé* ».

La présente politique présente des mesures de sécurité associées à l'utilisation du courrier électronique par les utilisateurs.

### **5. Énoncé de la politique :**

#### **Mesures de contrôle**

##### **5.1. Organisation de la sécurité**

Le CHUQ, par l'entremise de son directeur général, nomme une personne responsable de l'application de la présente politique laquelle agit à titre d'officier de sécurité informationnelle du CHUQ (ci-après désigné officier de sécurité informationnelle). Pour l'aider à réaliser son mandat, l'officier de sécurité informationnelle a créé un comité de sécurité informationnelle.

##### **5.2. Accès aux renseignements nominatifs, personnels ou confidentiels**

- Le CHUQ limite l'accès aux renseignements confidentiels. Lesdits renseignements ne sont accessibles que pour l'exercice des fonctions des seules personnes dont les tâches l'exigent et qui détiennent un privilège d'accès approprié.
- Les privilèges d'accès sont attribués par les personnes responsables, le tout conformément à un registre supervisé par l'officier de sécurité informationnelle mais tenu à jour par les responsables des accès.
- Toute personne qui reçoit un privilège d'accès s'engage à ne pas divulguer les renseignements confidentiels dont elle a pu prendre connaissance sauf dans le cadre de son travail. Dans le cas contraire, le CHUQ pourra imposer des sanctions disciplinaires ou administratives.
- À la demande du supérieur d'un utilisateur, l'officier de sécurité informationnelle, ou toute autre personne spécialement désignée par celui-ci, peut réviser, suspendre ou révoquer un privilège d'accès lorsque, entre autres raisons, la personne :

- quitte définitivement le CHUQ ou est congédiée;
- termine son contrat ou son assignation;
- change de fonctions à l'intérieur du CHUQ et que ses nouvelles fonctions n'exigent pas l'accès aux renseignements nominatifs, personnels ou confidentiels;
- s'absente pour une période déterminée par le CHUQ ou pour une période prolongée de plus de 90 jours; n'a pas utilisé son code d'accès, après vérification préalable, depuis plus d'un (1) an;
- divulgue des renseignements confidentiels pour des raisons autres que l'exercice de ses fonctions.

De plus,

- Pour tout comportement déviant ou usage abusif des systèmes d'informations constaté par l'officier de sécurité informationnelle celui-ci peut, entre autres, demander la révision, la suspension ou la révocation des privilèges d'accès.

### 5.3. *Utilisation d'Internet, d'intranet et des réseaux d'informations du CHUQ*

- Le CHUQ utilise des logiciels permettant de contrôler et d'enregistrer toute utilisation d'Internet faite à partir de ses réseaux d'informations. L'officier de sécurité informationnelle se réserve le droit d'enregistrer, peu importe l'utilisateur, toute page World Wide Web (www) visitée, tout clavardage ou bavardage en ligne (« chat ») ou forum de discussion (« newsgroup ») ou courrier électronique.
- Le CHUQ analyse et évalue en tout temps l'usage qui est fait d'Internet, de ses réseaux d'information et du RTSS<sup>MO</sup>.
- L'affichage de tout document ou tout graphique sexuellement explicite, haineux, raciste ou considéré inacceptable est interdit. De plus, de tels documents ne doivent pas être archivés, enregistrés, distribués ou édités par les réseaux d'informations du CHUQ.
- Il est interdit aux utilisateurs ou aux tiers de modifier les systèmes d'informations ni d'installer un actif informationnel sans autorisation préalable des personnes responsables désignées. Par exemple l'installation, et par conséquent l'utilisation, de jeux sur les systèmes d'informations n'est pas autorisée.
- Les actifs informationnels et de télécommunications, les outils Internet ou tous autres outils de travail qui sont accessibles par les réseaux d'informations du CHUQ ne doivent pas être en violation des lois et règlements en vigueur. L'usage d'Internet, des réseaux d'informations et des actifs informationnels et de télécommunications du CHUQ pour des activités illégales entraîne des mesures disciplinaires ou administratives pouvant aller jusqu'au congédiement. De plus, le CHUQ s'engage à coopérer face à toute requête provenant des forces de l'ordre ou à la demande de tout autre organisme mandaté à cet effet.
- Tout logiciel ou document téléchargé via Internet ou le RTSS<sup>MO</sup> vers les réseaux d'informations du CHUQ devient la propriété de celui-ci. Ils doivent être utilisés en accord avec leurs licences et leurs droits d'auteur.
- Aucun utilisateur ne peut utiliser les outils d'accès à Internet pour télécharger ou distribuer des données ou des logiciels piratés.

- Aucun utilisateur ne peut utiliser les outils d'accès à Internet pour propager quelque virus que ce soit sur les réseaux d'information du CHUQ ou tout autre réseau externe.
- Aucun utilisateur ne peut utiliser les outils d'accès à Internet ou au RTSS<sup>MO</sup> ou tout autre moyen pour rendre inutilisable ou surcharger quelque ordinateur ou réseau que ce soit ou encore pour contourner tout système mis en place pour protéger la vie privée ou la sécurité des autres utilisateurs.
- Aucun utilisateur des réseaux d'informations du CHUQ ne peut utiliser un modem sur son poste de travail sans l'approbation de l'officier de sécurité informationnelle.
- Seuls les utilisateurs dûment autorisés à intervenir, au nom du CHUQ, auprès des médias ou à des assemblées publiques peuvent participer au niveau des clavardages, bavardages en ligne « *chats* » et des forums de discussion ou « *newsgroups* ». Les autres utilisateurs peuvent participer à de tels groupes reliés à leur travail et en regard de leurs fonctions, mais ils le font en leur nom propre en tant qu'individu. Lors d'une telle participation, si un membre du personnel est identifié au CHUQ, il doit s'abstenir de tout commentaire ou endossement non autorisé.
- Tout utilisateur utilisant les outils d'accès à Internet doit s'identifier clairement et entièrement quand il participe à des clavardages, bavardages en ligne « *chats* » et à des forums de discussions « *newsgroups* » ou lorsqu'il sollicite un service auprès de systèmes externes;
- Le CHUQ conserve la propriété intellectuelle et les droits d'auteur de tous documents portés par ses systèmes d'informations, incluant tout matériel transmis à du clavardage, bavardage en ligne « *chat* » ou forum de discussion « *newsgroup* » ou page World Wide Web (www) créées par les membres de son personnel, ou d'un tiers, dans le cadre de leur travail.
- L'utilisation des outils d'accès à Internet, à partir du CHUQ, pour commettre des infractions telles qu'un usage abusif des actifs informationnels et de télécommunications, du harcèlement sexuel, la tenue d'un discours public non autorisé et le détournement ou le vol de la propriété intellectuelle sont également interdits.
- Les utilisateurs doivent planifier toutes opérations de téléchargements intensifs tels que les transferts de documents de grande taille, de documents vidéo ou sonores ou d'envois massifs de courrier électronique hors des heures régulières de travail, soit avant 08h30, entre 12h00 et 13h00 ou après 17h00.
- Tout document téléchargé doit être vérifié pour la présence de virus avant son exécution, sa lecture, son transfert, sa copie ou toute autre manipulation nécessitant son enregistrement sur quelque support des réseaux d'informations du CHUQ. L'utilisateur est responsable du contenu desdits documents en ce qui a trait aux virus qui pourraient s'y trouver. En conséquence, le CHUQ exige l'emploi de logiciels antivirus à jour sur les ordinateurs entrant en communication avec tous les réseaux d'informations.
- Les utilisateurs doivent respecter la confidentialité des connaissances, partielles ou totales, de la structure des réseaux d'information du CHUQ et ne peut divulguer, en tout ou en partie, cette information. De plus, les utilisateurs doivent s'assurer que leur utilisation des réseaux d'informations n'altère pas la structure de ceux-ci.

#### 5.4. Utilisation du courrier électronique

Tout utilisateur qui désire préserver le caractère confidentiel ou privé du contenu des courriers électroniques qu'il transmet doit utiliser des programmes ou autres techniques d'encryptage ou d'encodage mis à sa disposition sur le poste dont il se sert pour transmettre son courrier électronique. Par ailleurs, il doit également être conscient que les courriers électroniques qu'il envoie peuvent, à son insu, être redirigés, imprimés, sauvegardés ou affichés sur des médias ou des systèmes d'informations de tiers.

Le gestionnaire de système qui administre un système de courrier électronique doit fixer des règles concernant les délais de conservation des messages en vigueur au CHUQ. Les copies des messages, notamment celles que peut garder en mémoire le fournisseur de services Internet, sont soumises aux mêmes dispositions. Dans les organismes publics, les délais de conservation doivent être consignés dans un calendrier de conservation approuvé par les Archives nationales.

Le CHUQ attribue un privilège d'accès aux boîtes de courrier à l'administrateur Lotus Notes<sup>MC</sup> et à l'officier de sécurité informationnelle. Ces droits sont effectifs, pour l'administrateur Notes, seulement pour la réexpédition de messages qui ne sont pas arrivés à destination. L'officier de sécurité informationnelle peut faire la surveillance du contenu des messages et la détection de fraude pour fin d'enquête ou sur mandat des autorités.

Puisqu'il est ici question de l'utilisation du courrier électronique en milieu de travail, le CHUQ s'accorde un droit de surveillance du trafic des boîtes de courrier. L'utilisation du courrier électronique fait l'objet de règles strictes énoncées dans le Code de conduite des utilisateurs et fourni en annexe.

Plus particulièrement, concernant le courrier électronique les précautions élémentaires suivantes doivent être appliquées. Entre autres :

- l'accès aux boîtes de courrier est restreint et protégé par un mot de passe;
- l'utilisateur devra modifier son mot de passe tous les 120 jours. Le mot de passe doit être composé de chiffres et de lettres et contenir au moins 8 caractères;
- si l'utilisateur fait une erreur en tapant son mot de passe trois fois de suite, l'utilisation du poste sera automatiquement suspendue si le logiciel le permet;
- à chaque boîte postale correspond un mot de passe géré par la personne autorisée à y accéder;
- dans le cas d'une boîte commune, seuls les membres du personnel autorisé à y accéder doivent connaître le mot de passe;
- le système doit posséder un mécanisme de gestion des mots de passe selon le profil de l'utilisateur. De plus, l'historique des dix (10) derniers mots de passe est conservé;
- le mot de passe n'est pas affiché lorsqu'il est saisi par l'utilisateur;
- un logiciel d'économie d'écran qui redemande le mot de passe après une courte période d'inactivité doit être installé sur chaque ordinateur;
- l'usage du courrier électronique doit être limité aux messages et aux fichiers qui ont rapport au travail;
- l'usage du courrier électronique est interdit pour des fins syndicales;
- la modification d'un message avant sa retransmission à un autre destinataire est interdite.

Comme précaution supplémentaire pour assurer la confidentialité des messages et fichiers expédiés par courrier électronique, l'encodage ou l'encryptage est recommandé. Si s'agit d'une méthode d'encryptage autre que le chiffrement mis à sa disposition, l'utilisation d'un outil spécialisé autre devra être autorisée au préalable par l'officier de sécurité informationnelle.

S'il ne peut assurer l'encryptage ou l'encodage d'un document à caractère confidentiel, l'utilisateur devra employer un autre moyen de communication pour acheminer ledit document ou obtenir l'autorisation de son supérieur immédiat.

### **5.5. Utilisation du télétravail**

Le contrôle de l'utilisation du télétravail est fait par l'officier de sécurité informationnelle ou une personne déléguée par celui-ci selon les exigences du RTSS<sup>MO</sup>.

Seules les personnes expressément autorisées au préalable par leurs supérieurs immédiats à utiliser le télétravail ont accès aux services ou aux logiciels qui leur seront explicitement autorisés par l'officier de sécurité informationnelle selon des modalités précises.

### **5.6. Utilisation des technologies sans fils**

L'utilisation des technologies sans fils, ordinateurs de poches ou tout autre type d'équipements de type point d'accès, *Pocket PC<sup>MC</sup>*, *Palm Pilot<sup>MC</sup>* ou de tout autre technologie qui pourrait être disponible n'est pas autorisée sur les réseaux du CHUQ à moins d'entente préalable avec l'officier de sécurité informationnelle ou d'une personne déléguée par celui-ci et selon des modalités précises.

### **5.7. Copies de sécurité**

Des règles et procédures concernant la prise des copies de sécurité, leur conservation, la récupération et la destruction de celles-ci sont établies par l'officier de sécurité informationnelle. Toutes les copies de sécurité doivent être entreposées dans un endroit sécuritaire. Les procédures concernant la destruction et la conservation de ces copies doivent être élaborées par le CHUQ. ***Copies de source externe***

Tout document informatique de source externe et quel que soit son support doit être vérifié contre les virus avant son exécution ou sa utilisation. S'il y a présence d'un virus ou si on a un doute raisonnable de croire qu'il y en a un, il est formellement interdit d'utiliser ce document informatique dans les appareils du CHUQ.

### **5.9. Développement et conception d'applications et projets d'informatisation**

Tout projet de développement et de conception d'applications, projet d'informatisation ou de mise en œuvre doit tenir compte des obligations réglementaires et normatives en matière de sécurité des actifs informationnels.

### **5.10. Gestions des documents**

Tout document contenant des renseignements confidentiels, doit être conservé et détruit de manière sécuritaire.

### **5.11. Utilisation des imprimantes et des télécopieurs**

Toute personne qui achemine ou imprime un document contenant des renseignements à caractère confidentiel doit assurer la confidentialité de celui-ci.

L'imprimante ou le télécopieur doivent être placés de façon à éviter toute utilisation et observation non autorisées, donc dans un endroit surveillé et non accessible au public. S'il s'agit d'un périphérique,

celui-ci doit être utilisé par les personnes autorisées par le détenteur de l'actif informationnel, selon les privilèges d'accès consentis à l'utilisateur. Les documents doivent faire l'objet d'une surveillance et être rangés dans un endroit sûr et non accessible facilement par le public.

En ce qui a trait plus particulièrement à l'utilisation du télécopieur, l'utilisateur doit, en tout temps :

- vérifier, avant la transmission, si les renseignements nominatifs ou confidentiels qu'il contient peuvent être extraits;
- remplir un formulaire d'accompagnement indiquant les renseignements, nom, adresse ou société ou firme, ainsi que no. de téléphone et de télécopieur concernant le destinataire ainsi que l'identification de l'expéditeur ainsi que le numéro de téléphone de celui-ci;
- vérifier si le numéro de téléphone composé dans la fenêtre du télécopieur correspond au numéro du destinataire et annuler l'envoi en cas d'erreur;
- vérifier le rapport de transmission ou de non réussite à la fin de la communication;
- vérifier auprès du destinataire si les documents transmis ont été bien reçus.

De plus, s'il s'agit de la transmission de renseignements confidentiels, l'utilisateur doit, en plus de ce qui précède :

- vérifier le degré d'urgence de communiquer des renseignements confidentiels;
- indiquer visiblement le caractère confidentiel;
- aviser le destinataire de l'heure de la transmission et s'assurer de sa présence, ou de la présence d'une personne déléguée, au moment de la réception;
- obtenir la confirmation de la réception de l'envoi par la personne autorisée à recevoir la communication.

Pour ces envois spécifiques le rapport de transmission peut être conservé par l'expéditeur.

### **5.12. Sécurité des télécommunications**

Le CHUQ a mis en place des infrastructures réseaux sécurisées intégrant les accès, les protocoles de communication, les systèmes d'exploitation et les équipements, et prend les mesures appropriées pour assurer la disponibilité, l'intégrité, la confidentialité, l'authentification et l'irrévocabilité des données.

### **5.13. Mesures de sécurité**

Les principes de sécurité s'articulent autour des responsabilités particulières en matière de sécurité lesquels reposent sur une approche globale et une compréhension des divers intervenants sur cette notion de sécurité des actifs informationnels. Des mesures de contrôle, de protection et de prévention sont appliquées.

Le CHUQ, par l'officier de sécurité informationnelle, par la DRH à l'embauche, par ses gestionnaires s'il y a lieu, ou par toute autre personne désignée, fait signer un engagement de confidentialité à toute personne tel que désigné à l'article 3 de la présente politique, aux tiers, et au personnel de ses fournisseurs de services et à toutes les personnes qui font l'objet d'un prêt de services, qui effectuent de la sous-traitance et/ou qui effectuent des tâches pour le CHUQ. Les contrats de services et ententes devront préciser les exigences en matière de sécurité.

#### **5.14. Évaluation de la sécurité**

Des vérifications informatiques et des audits sont effectués pour vérifier le respect des mesures, pratiques et procédures relatives à la sécurité des actifs informationnels et des mesures sont prises afin d'apporter un suivi.

#### **5.15. Programme d'information, de sensibilisation et de formation du personnel**

Le CHUQ a mis en œuvre un programme d'information, de sensibilisation et de formation du personnel dans le but de l'informer de ses responsabilités et de la nécessité de protéger l'accès aux données sociosanitaires confidentielles et d'assurer la sécurité concernant l'utilisation des actifs informationnels et de télécommunications.

#### **5.16. Manquements à la sécurité**

L'officier de sécurité informationnelle doit faire enquête sur tout manquement à la sécurité informatique et appliquer les mesures correctrices qui s'imposent au niveau informatique. Il doit aussi faire rapport au supérieur immédiat de l'utilisateur, selon des modalités prédéterminées et approuvées par le CHUQ, et à la direction des ressources humaines qui prendront les mesures administratives ou disciplinaires pour toute contravention à la politique ou pour toute mauvaise utilisation des réseaux d'informations du CHUQ.

Tout membre du personnel qui contrevient au code de conduite, à la présente politique et à la réglementation qui en découle est passible des sanctions suivantes:

Notamment :

- mesures administratives et disciplinaires ou autres sanctions appropriées à l'intention du personnel conformément aux lois et règlements en vigueur et aux conventions collectives de travail;
- révocation de certains privilèges d'accès aux équipements et services visés par la présente politique;
- remboursement au CHUQ de toute somme, y compris les sommes émanant d'un jugement prononcé par tout tribunal ou organisme réglementaire quelconque à l'endroit du CHUQ et qui découlerait de l'utilisation non autorisée, frauduleuse ou illicite de ses services ou de ses actifs informationnels et de télécommunications ou de ses systèmes d'informations.

#### **5.17. Mise à jour de la politique**

La présente politique doit être périodiquement révisée, au moins aux trois (3) ans, afin de tenir compte du cadre légal s'il y a lieu, des nouvelles pratiques et technologies utilisées au CHUQ ainsi qu'aux besoins exprimés.

Toute modification à la présente politique doit être adoptée par le conseil d'administration du CHUQ, sauf pour les annexes et pour se conformer à la Loi.

Les annexes, telles les différents codes de conduite, les formulaires ou autres documents nécessaires à la gestion et rédigés en conformité avec ladite politique, peuvent faire l'objet d'ajustements pour les rendre

conformes aux technologies utilisées ou aux circonstances motivant la modification. Elles font cependant partie intégrante de la politique.

### **5.18. Rôles et responsabilités du CHUQ**

Cette section vise à établir les rôles et responsabilités de chacun selon les fonctions qu'il occupe au sein du CHUQ en ce qui a trait à la sécurité des actifs informationnels.

#### **5.18.1. Le conseil d'administration**

Le conseil d'administration:

- approuve la présente politique;
- s'assure de la mise en œuvre de la présente politique;
- fait le suivi de l'application de la présente politique;
- approuve le plan d'action;
- entérine la nomination de l'officier de sécurité informationnelle;
- entérine le bilan annuel concernant la sécurité des actifs et le transmet au coordonnateur de la sécurité au niveau supérieur, soit la RRSSS de Québec.

#### **5.18.2. Le directeur général**

Le directeur général assume les responsabilités suivantes:

- assure l'application de la politique dans l'organisation ;
- apporte les appuis financiers et logistiques nécessaires pour la mise en œuvre et l'application de la présente politique;
- soumet le bilan annuel concernant l'application de la politique au conseil d'administration;
- informe et mobilise les gestionnaires et le personnel concernant l'application de la politique;
- nomme l'officier de sécurité informationnelle et les assistants de la sécurité, leur fait connaître leurs responsabilités et leur délègue les pouvoirs requis pour appliquer la présente politique.

#### **5.18.3. L'officier de sécurité informationnelle**

L'officier de sécurité informationnelle est le responsable de la sécurité des actifs informationnels du CHUQ.

En collaboration avec les gestionnaires et plus particulièrement avec le directeur adjoint des finances et des systèmes d'information de gestion, dans le cadre de l'exercice de son mandat, il:

- élabore et met à jour la politique sur la sécurité des actifs informationnels, la soumet au directeur général et au conseil d'administration pour approbation;
- préside le comité de sécurité informationnelle;
- établit un programme général d'application et de respect de la présente politique en concordance avec les orientations régionales;
- fait connaître l'importance de l'application de celle-ci et identifie avec les gestionnaires les détenteurs d'actifs informationnels;
- met en œuvre, participe et élabore un programme général d'information, de sensibilisation et de formation dans le but d'informer le personnel, et les tiers, le cas échéant;
- gère les aspects relatifs à l'escalade des incidents de sécurité et procède à des évaluations de la situation en matière de sécurité;
- s'assure que toutes les directions du CHUQ acquièrent les équipements et le matériel nécessaires pour appliquer la présente politique, propose des solutions et coordonne la mise en place de ces solutions;
- produit un bilan annuel, ayant trait à l'application de la Politique; par la suite il met en œuvre les actions pour apporter les correctifs qui s'imposent suite à la parution du bilan annuel;
- prévoit annuellement et au besoin, les bilans et rapports relatifs à la sécurité des actifs informationnels du CHUQ en s'assurant que l'information sensible à diffusion restreinte soit traitée de manière confidentielle, et après approbation par le directeur général et le conseil d'administration, le soumet au coordonnateur régional de la sécurité des actifs informationnels de la région de Québec;
- coordonne toutes les activités reliées à la protection des renseignements confidentiels ou sociosanitaires et à la sécurité concernant les actifs informationnels et des télécommunications;
- autorise l'utilisation de certains équipements spécialisés selon les normes de sécurité reconnues, le tout en relation avec la mission ou les mandats du CHUQ;
- vérifie périodiquement que le programme général de sécurité concernant les actifs informationnels et des télécommunications et de protection des renseignements confidentiels ou données sociosanitaires soit respecté et suit la mise en œuvre de toute recommandation découlant d'une vérification ou d'un audit;
- élabore des ententes avec les fournisseurs de services, ou entre établissements ou organismes, afin de respecter les lois et les règlements en vigueur au Québec concernant la confidentialité des données confidentielles ou sociosanitaires et l'utilisation des technologies de l'information.

De plus, pour un ou des mandats spécifiques, l'officier de sécurité informationnelle peut établir des mesures plus strictes que celles prévues à la présente politique.

#### **5.18.4. *Le gestionnaire du personnel utilisateur***

Chaque gestionnaire agit à titre de détenteur d'actifs informationnels qui leur sont confiés. Chacun:

- applique la présente politique au niveau de la direction ou du secteur d'activités dont il a la gestion;
- contribue à la production du bilan annuel (suivi et contrôle) de l'application de la Politique;
- applique les sanctions prévues à la présente politique lors d'un manquement à la sécurité de la part d'un membre du personnel faisant partie de sa direction ou de son secteur d'activités;
- diffuse l'importance de l'application de la présente politique au niveau de sa direction ou de son secteur d'activités et en assure le suivi;
- assure la sécurité d'un ou de plusieurs actifs informationnels qui leur sont confiés;
- s'implique dans l'ensemble des activités relatives à la sécurité;
- détermine les règles d'accès aux actifs dont il assume la responsabilité avec l'appui de l'officier de sécurité informationnelle;
- s'assure que les mesures de sécurité appropriées sont élaborées, approuvées, mises en place et appliquées systématiquement dans son secteur d'activités;
- est responsable du plan de continuité de son secteur d'activités en cas de non accessibilité aux systèmes d'information;
- assumer la responsabilité, donc l'imputabilité des manquements possibles à la présente politique par son rôle et à son niveau de responsabilités.

#### **5.18.5. *Le comité de sécurité informationnelle***

Le comité de sécurité informationnelle recommande à l'officier de sécurité informationnelle des mesures de sécurité et des règles de confidentialité pour assurer la protection des données et des renseignements confidentiels et la sécurité des actifs informationnels et de l'infrastructure nécessaire à leur maintien.

#### **5.18.6. *Le responsable de l'application de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels***

Veille au respect de la Loi et, pour ce faire, collabore avec l'officier de sécurité informationnelle à toutes les étapes du cycle de vie de l'information.

#### **5.18.7. *Les utilisateurs***

Les utilisateurs:

- sont informés de l'existence de la Politique et y adhèrent;

- appliquent et respectent les lois et règlements qui régissent leur domaine d'activités ainsi que toutes les politiques, mesures et procédures en matière de sécurité dont la présente politique et les différents codes de conduite qui leur sont assujettis en tous points;
- doivent respecter le caractère confidentiel des renseignements contenus dans des documents auxquels ils auraient pu avoir accès même par mégarde;
- avisent leur supérieur immédiat de toute situation portée à leur connaissance et qui est susceptible de compromettre la sécurité des actifs informationnels du CHUQ;
- assumer la responsabilité, donc l'imputabilité des manquements possibles à la présente politique par son rôle et à son niveau de responsabilités.

**5.19. *Engagement de confidentialité par les tiers ou le personnel des fournisseurs de services du CHUQ***

Tous les membres du personnel des fournisseurs de services du CHUQ qui ont accès, de près ou de loin, à des documents, qu'ils soient confidentiels ou non, et aux actifs informationnels et de télécommunications, doivent signer un engagement de confidentialité avec le CHUQ ou le secteur concerné par le service demandé.

Par ce document, les tiers s'engagent formellement à respecter la présente politique et plus spécifiquement le ou les codes de conduite qui accompagnent ladite politique et qui les concernent.

**6. *Mise en application***

La version amendée de la présente politique entre en vigueur dès son approbation par le conseil d'administration du CHUQ.

**A**

**N**

**N**

**E**

**X**

**E**

**S**

## Annexe I –Engagement de confidentialité type

*Je, par la présente, (nom) \_\_\_\_\_ (prénom) \_\_\_\_\_  
(fonction ou titre d'emploi) \_\_\_\_\_  
(nom et adresse de l'employeur) \_\_\_\_\_,*  
*confirme avoir été informé(e) de l'existence de la Politique en matière de sécurité informationnelle du Centre hospitalier universitaire de Québec ( CHUQ) dont le texte intégral est disponible sur demande en format papier à la DRH, auprès de mon chef de service, sur le réseau Internet ([www.chuq.qc.ca](http://www.chuq.qc.ca)) sous l'onglet Politiques et sur l'intranet du CHUQ sous la rubrique DFSIG/SSIG/Sécurité informationnelle/Documents à consulter.*

*Je m'engage à prendre connaissance de cette politique, à y adhérer et à la respecter ainsi que les codes de conduite applicables. Je dois en tout temps prendre toutes les mesures mises à ma disposition afin d'appliquer cette politique dans l'exercice de mes fonctions et des tâches qui y sont associées.*

*J'ai le devoir d'informer immédiatement mon supérieur immédiat de tout incident ou toute situation portée à ma connaissance qui serait susceptible de compromettre la confidentialité des renseignements confidentiels et la sécurité concernant l'utilisation des actifs informationnels et de télécommunications.*

*Je m'engage à ne jamais dévoiler des renseignements susceptibles de mettre en péril soit la confidentialité des renseignements confidentiels et des données sociosanitaires, soit la sécurité des actifs informationnels et de télécommunications du CHUQ.*

*Je suis pleinement conscient(e) que le CHUQ utilise des logiciels de sécurité qui peuvent enregistrer, pour des fins de gestion, le contenu de mon courrier électronique, les adresses Internet des sites que je visite et conserver un dossier de toute activité réalisée sur ses réseaux d'information au cours de laquelle je transmets ou reçois quelque document que ce soit lorsque j'utilise les systèmes d'informations et ressources du CHUQ.*

*J'ai été informé(e) que le CHUQ peut enregistrer et archiver les messages que je reçois ou envoie pour des fins de gestion et peut me soumettre, de manière ponctuelle, à un audit ou à une vérification informatique si requis par l'officier de sécurité informationnelle du CHUQ. J'ai été informé(e) également qu'il pourrait y avoir des mesures administratives ou disciplinaires prises à mon égard dans le cas où je manquerais à mes engagements.*

---

Signature du membre du personnel  
Prénom et nom

---

Date

Numéro d'employé(e)  
du CHUQ : \_\_\_\_\_

---

Signature du représentant du CHUQ  
Prénom et nom

---

Date

Original au dossier

**Annexe II - Déclaration de l'employé(e) quant à la connaissance et au respect de la  
Politique en matière de sécurité informationnelle**

---

*Je, par la présente, (nom) \_\_\_\_\_ (prénom) \_\_\_\_\_  
(fonction ou titre d'emploi) \_\_\_\_\_  
(nom et adresse de l'employeur) \_\_\_\_\_,  
déclare avoir participé à une séance d'information à l'occasion de laquelle la Politique en matière de  
sécurité informationnelle du Centre hospitalier universitaire de Québec (CHUQ) m'a été remise et  
expliquée. Le texte intégral de cette politique est disponible sur demande en format papier à la DRH,  
auprès de mon chef de service, sur Internet à l'adresse suivante: [www.chuq.qc.ca](http://www.chuq.qc.ca) sous l'onglet  
Politiques et sur l'intranet du CHUQ sous la rubrique DFSIG/SSIG/Sécurité  
informationnelle/Documents à consulter.*

*Je m'engage à y adhérer et à respecter cette politique ainsi que les codes de conduite applicables. Je  
dois en tout temps prendre toutes les mesures mises à ma disposition afin d'appliquer cette politique  
dans l'exercice de mes fonctions et des tâches qui y sont associées.*

*J'ai le devoir d'informer immédiatement mon supérieur immédiat de tout incident ou toute situation  
portée à ma connaissance susceptible de compromettre la confidentialité des renseignements  
confidentiels et la sécurité concernant l'utilisation des actifs informationnels et de télécommunications.*

*Je m'engage à ne jamais dévoiler des renseignements susceptibles de mettre en péril soit la  
confidentialité des renseignements confidentiels et des données sociosanitaires, soit la sécurité des actifs  
informationnels et de télécommunications du CHUQ.*

*Je suis pleinement conscient(e) que le CHUQ utilise des logiciels de sécurité qui peuvent enregistrer,  
pour des fins de gestion, le contenu de mon courrier électronique, les adresses Internet des sites que je  
visite et conserver un dossier de toute activité réalisée sur ses réseaux d'information au cours de laquelle  
je transmets ou reçois quelque document que ce soit lorsque j'utilise les systèmes d'informations et  
ressources du CHUQ.*

*J'ai été informé(e) que le CHUQ peut enregistrer et archiver les messages que je reçois ou envoie pour  
des fins de gestion et peut me soumettre, de manière ponctuelle, à un audit ou à une vérification  
informatique si requis par l'officier de sécurité informationnelle du CHUQ. J'ai été informé(e)  
également qu'il pourrait y avoir des mesures administratives ou disciplinaires prises à mon égard dans le  
cas où je manquerais à mes engagements.*

---

Signature du membre du personnel  
Prénom et nom

---

Date

Numéro d'employé(e)  
du CHUQ : \_\_\_\_\_

---

Signature du représentant du CHUQ  
Prénom et nom

---

Date

Original au dossier

### **Annexe III - Code de conduite des utilisateurs**

---

Le présent code de conduite a été conçu dans le but de faciliter l'application de la Politique en matière de sécurité informationnelle du CHUQ. Il doit être respecté et appliqué par tous les membres du personnel du CHUQ qui utilisent ou qui gèrent des renseignements confidentiels et des actifs informationnels ou de télécommunications et à tous les tiers qui peuvent avoir accès aux actifs informationnels du CHUQ tel que défini dans la présente politique. Le texte intégral de cette politique est disponible sur le site du CHUQ à l'adresse suivante : [www.chuq.qc.ca](http://www.chuq.qc.ca) sous la rubrique *Politiques* et sur l'intranet du CHUQ sous la rubrique DFSIG/SSIG/Sécurité informationnelle/

#### **Responsabilités de l'utilisateur**

##### ***Tout utilisateur doit :***

- appliquer et respecter les lois et règlements qui régissent leur domaine d'activités ainsi que toutes les politiques, mesures et procédures en matière de sécurité, dont la présente politique et les différents codes de conduite qui leur sont assujettis en tous points;
- utiliser les actifs informationnels selon les normes permises;
- aviser leur supérieur immédiat de toute situation portée à leur connaissance et qui est susceptible de compromettre la sécurité des actifs informationnels du CHUQ;
- utiliser que les codes d'utilisateur ainsi que les mots de passe pour lesquels il a obtenu une autorisation d'usage et ne pas les divulguer;
- assumer entièrement la responsabilité des activités résultant de l'usage de ses codes d'utilisateurs ainsi que de ses mots de passe;
- prendre des mesures raisonnables afin de protéger ses codes d'utilisateurs, ses mots de passe ainsi que l'intégrité et la confidentialité des actifs informationnels utilisés;
- s'abstenir d'utiliser les systèmes d'informations ou de télécommunications à des fins non autorisées, syndicales, commerciales ou illégales;
- obtenir l'autorisation des personnes concernées pour accéder, modifier, reproduire, détruire ou lire des informations, des programmes ou des logiciels;
- respecter le caractère confidentiel des données sociosanitaires nominatives, ou des documents auxquels il a accès lors de l'exercice de ses fonctions ;
- respecter le caractère confidentiel des renseignements contenus dans des documents auxquels ils auraient pu avoir accès même par mégarde;
- respecter le droit d'auteur des logiciels, des informations et de la documentation utilisés;
- s'assurer que tout document à caractère confidentiel, quel que soit son support, soit hors d'atteinte en les rangeant en lieu sûr;

• **Annexe III - Code de conduite des utilisateurs** (suite)

---

- s'assurer que son poste informatique, s'il travaille sur les réseaux d'informations reste ouvert la nuit pour le passage de l'antivirus ou, s'il travaille sur un poste local, vérifier que son logiciel antivirus soit fonctionnel;
- voir au respect des règles de sécurité par toute personne de l'extérieur qui vient dans les locaux à titre de visiteur;
- avertir son supérieur immédiat s'il possède de l'information concernant tout mécanisme pour détourner ou contrer les systèmes de sécurité mis en place au CHUQ et ne pas utiliser ou diffuser, ledit mécanisme;
- respecter l'interdiction d'utiliser les outils d'accès à Internet ou le RTSS<sup>MO</sup> pour télécharger ou distribuer des données ou des logiciels piratés ou encore pour propager quelque virus que ce soit sur les réseaux d'information du CHUQ ou tout autre réseau externe;
- respecter l'interdiction d'utiliser les outils d'accès à Internet ou au RTSS<sup>MO</sup>, ou tout autre moyen, pour rendre inutilisable ou surcharger quelque ordinateur ou réseau que ce soit ou pour contourner tout système mis en place pour protéger la vie privée ou la sécurité des autres utilisateurs;
- respecter l'interdiction d'utiliser un modem sur son poste de travail sans l'approbation de l'officier de sécurité informationnelle du CHUQ;
- planifier toute opération de téléchargements intensifs tels que les transferts de documents de grande taille, de documents vidéos ou sonores ou d'envois massifs de courrier électronique hors des heures régulières de travail, soit avant 8 h 30, entre 12 h et 13 h ou après 17 h;
- vérifier tout document téléchargé pour la présence de virus avant son exécution, sa lecture, son transfert, sa copie ou toute autre manipulation nécessitant son enregistrement sur quelque support des réseaux d'informations du CHUQ. L'utilisateur est responsable du contenu desdits documents en ce qui a trait aux virus qui pourraient s'y trouver. En conséquence, le CHUQ exige l'emploi de logiciels antivirus à jour sur les ordinateurs entrant en communication avec tous les réseaux d'informations du CHUQ;
- respecter la confidentialité des connaissances, partielles ou totales, de la structure des réseaux d'information du CHUQ et ne peut divulguer, en tout ou en partie, cette information. De plus, les utilisateurs doivent s'assurer que leur utilisation des réseaux d'informations n'altère pas la structure de ceux-ci;
- utiliser les outils d'accès à Internet en s'identifiant clairement et entièrement quand il participe à du bavardage en ligne « chats » et à des forums de discussion « newsgroups » ou lorsqu'il sollicite un service auprès de systèmes externes;
- être autorisé au préalable pour intervenir, au nom du CHUQ, auprès des médias ou à des assemblées publiques. Il peut alors le faire au niveau du clavardage, bavardage en ligne « chats » et à des forums de discussion « newsgroups »;

• **Annexe III - Code de conduite des utilisateurs** (suite)

---

- respecter l'interdiction de modifier les systèmes d'informations ou d'installer un actif informationnel sans autorisation préalable des personnes responsables désignées. Par exemple, l'installation, et par conséquent l'utilisation, de jeux sur les systèmes d'informations n'est pas autorisée;
- respecter l'interdiction d'utiliser des technologies sans fils, ordinateurs de poches ou tout autre type d'équipements de type point d'accès, *Pocket PC<sup>MC</sup>*, *Palm Pilot<sup>MC</sup>* ou de tout autre technologie qui pourrait être disponible à moins d'entente préalable avec l'officier de sécurité informationnelle ou d'une personne déléguée par celui-ci et selon des modalités précises;
- respecter le caractère confidentiel des renseignements contenus dans des documents auxquels ils auraient pu avoir accès même par mégarde;
- assumer la responsabilité, donc l'imputabilité des manquements possibles à la présente politique par son rôle et à son niveau de responsabilités.

De plus, tout utilisateur doit:

- préserver le caractère confidentiel ou privé du contenu des courriers électroniques qu'il transmet en utilisant des programmes ou autres techniques d'encryptage ou d'encodage sur le poste dont il se sert pour transmettre son courrier électronique si nécessaire, tel le chiffrement de Lotus Notes<sup>MC</sup>. Par ailleurs, il doit également être conscient que les courriers électroniques qu'il envoie peuvent, à son insu, être redirigés, imprimés, sauvegardés ou affichés sur des médias ou des systèmes d'informations de tiers;
- respecter le droit à la vie privée des autres utilisateurs des réseaux et des systèmes de télécommunications notamment en ce qui a trait à l'utilisation et à l'accès au contenu du courrier électronique, des boîtes vocales, de la téléphonie ou tout autre média de communications;
- respecter les conventions d'accès et d'usage des réseaux internes et externes, et identifier correctement sa correspondance électronique;
- éviter l'affichage de tout document ou tout graphique sexuellement explicite, haineux, raciste ou considéré inacceptable. De plus, de tels documents ne doivent pas être archivés, enregistrés, distribués ou édités par les réseaux d'informations du CHUQ;
- collaborer avec les gestionnaires de réseaux ou de systèmes d'informations afin de faciliter l'identification et la correction de problèmes ou d'anomalies pouvant se présenter;
- informer le responsable du réseau ou du système concerné de tout usage non autorisé des codes d'utilisateurs et des mots de passe;
- éviter tout comportement nocif ou malveillant tels que les suivants, cités à titre d'exemples:
  - intrusion ou tentative d'intrusion non autorisée dans un poste de travail, dans un système ou dans un réseau interne ou externe;
  - tentative de lire ou de copier des informations ou d'accéder à des fonctions ou des informations auxquelles ils n'ont pas droit, même si ces dernières sont physiquement accessibles;

### Annexe III - Code de conduite des utilisateurs (suite)

---

- usage volontaire de programmes ou autres moyens qui endommagent les actifs informatiques ou de télécommunication ou leur contenu (ex. : virus informatiques);
- usage de programmes, de logiciels ou autres moyens en vue d'intercepter, de collecter, de prendre connaissance, de décrypter ou de décoder de l'information (ex. : code d'utilisateur, clé d'accès, fichier ou mots de passe) véhiculée sur un réseau ou résidant sur un poste de travail;
- usage de subterfuges ou de moyens pour transmettre du courrier électronique de façon anonyme, pour usurper l'identité d'un usager ou en masquant son identité;
- utilisation du courrier électronique ou de la messagerie vocale pour véhiculer des messages ou des propos obscènes, haineux, racistes, diffamatoires, harcelants ou pour commettre tout autre acte réprimé par la loi ou par les règlements du CHUQ;
- utilisation sans autorisation du code de l'utilisateur ou du code d'accès ainsi que du mot de passe d'un tiers;
- lecture, modification, destruction ou diffusion non autorisée d'informations, de programmes ou de logiciels appartenant à un tiers;
- interférence volontaire en vue de dégrader la performance d'un poste de travail, d'un système ou d'un réseau informatique;
- usage du courrier électronique pour participer à une chaîne de lettres, pour effectuer de la publicité ou de la vente pyramidale ou encore pour faire des envois massifs de messages sans autorisation ou à des fins personnelles;
- usage des technologies sans fils, ordinateurs de poches ou tout autre type d'équipements de type point d'accès, *Pocket PC<sup>MC</sup>*, *Palm Pilot<sup>MC</sup>* ou de tout autre technologie qui pourrait être disponible sur les réseaux du CHUQ sans entente préalable avec l'officier de sécurité informationnelle ou d'une personne déléguée par celui-ci.

Concernant le courrier électronique, plus particulièrement, les précautions élémentaires suivantes doivent être appliquées:

- l'accès aux boîtes de courrier est restreint et protégé par un mot de passe;
- l'utilisateur devra modifier son mot de passe tous les 120 jours. Le mot de passe doit être composé de chiffres et de lettres et contenir au moins 8 caractères;
- si l'utilisateur fait une erreur en tapant son mot de passe trois fois de suite, l'utilisation du poste sera automatiquement suspendue si le logiciel le permet;
- à chaque boîte postale correspond un mot de passe géré par la personne autorisée à y accéder;
- dans le cas d'une boîte commune, seuls les membres du personnel autorisé à y accéder doivent connaître le mot de passe;
- le système doit posséder un mécanisme de gestion des mots de passe selon le profil de l'utilisateur. De plus, l'historique des dix (10) derniers mots de passe est conservé;
- le mot de passe n'est pas affiché lorsqu'il est saisi par l'utilisateur;
- un logiciel d'économie d'écran qui redemande le mot de passe après une courte période d'inactivité doit être installé sur chaque ordinateur;
- l'usage du courrier électronique doit être limité aux messages et aux fichiers qui ont rapport au travail;
- l'usage du courrier électronique est interdit pour des fins syndicales;
- l'usage du courrier électronique pour participer à une chaîne de lettres, pour effectuer de la publicité ou de la vente pyramidale ou encore pour faire des envois massifs de messages sans autorisation ou à des fins personnelles est interdit;
- la modification d'un message avant sa retransmission à un autre destinataire est interdite.

## **Annexe IV - Code de conduite des informaticiens et administrateurs des réseaux d'informations**

Le présent code de conduite a été conçu dans le but de faciliter l'application de la Politique en matière de sécurité informationnelle du CHUQ (ci-après désignée Politique). Il doit être respecté et appliqué par tous les membres du personnel du CHUQ qui utilisent ou qui gèrent des renseignements confidentiels et des actifs informationnels ou de télécommunications et par tous les tiers qui peuvent avoir accès aux actifs informationnels du CHUQ tel que défini dans la présente politique. Le texte intégral de cette Politique est disponible sur le site du CHUQ à l'adresse suivante : [www.chuq.qc.ca](http://www.chuq.qc.ca) sous la rubrique *Politiques*.

En plus de respecter et adhérer au code de conduite des utilisateurs, toute personne responsable de la gestion du matériel informatique ou des réseaux d'informations ou d'un système d'informations a des obligations envers les utilisateurs. En particulier, elle:

- administre le matériel informatique, le réseau d'information ou le système d'information de manière licite et efficace;
- respecte le caractère confidentiel de l'information emmagasinée par les utilisateurs ou leur appartenant en propre lors de toute intervention de gestion;
- respecte le caractère confidentiel des renseignements contenus dans des documents auxquels elle aurait pu avoir accès même par mégarde;
- prend des mesures adéquates afin que les utilisateurs puissent travailler dans un environnement garantissant la sécurité et la confidentialité des informations;
- informe les utilisateurs des conventions d'usage et de protection des informations concernant le matériel informatique, les réseaux d'informations ou les systèmes d'information;
- prévient la modification, la corruption et la reproduction illicite des informations, des programmes et des logiciels (incluant la documentation) sous sa responsabilité;
- prend des mesures raisonnables afin d'améliorer, en fonction des besoins, la sécurité des actifs informationnels et de télécommunications, notamment par l'installation des correctifs ou améliorations fournis par les producteurs de logiciels ou par les manufacturiers d'équipements;
- s'assure que les personnes non autorisées n'aient pas accès au matériel informatique, aux réseaux d'informations, à un système informatique et aux lieux dont l'accès est interdit;
- obtient l'autorisation de l'officier de sécurité informationnelle du CHUQ avant de procéder à un test de sécurité.
- informe son supérieur immédiat de tout manquement ou de toute situation portée à sa connaissance pouvant contrevenir à la *Politique en matière de sécurité informationnelle* du CHUQ et au présent code de conduite, et collabore aux suites à donner;
- rend accessible aux utilisateurs, dans des délais raisonnables, le matériel informatique ou les réseaux d'informations dont ils ont besoin dans l'exercice de leurs fonctions;
- utilise des données fictives ou dénominalisées lors de la formation des utilisateurs ou de démonstrations de systèmes;
- assume la responsabilité, donc l'imputabilité des manquements possibles à la présente politique par son rôle et à son niveau de responsabilités.

## **Annexe V - Code de conduite du personnel des fournisseurs de services ou d'un tiers**

---

Le présent code de conduite a été conçu dans le but de faciliter l'application de la *Politique en matière de sécurité informationnelle* du CHUQ (ci-après désignée Politique). Il doit être respecté et appliqué par tous les membres du personnel du CHUQ qui utilisent ou qui gèrent des renseignements confidentiels et des actifs informationnels ou de télécommunication et par tous les tiers qui ont accès aux actifs informationnels du CHUQ tel que défini dans la présente politique. Le texte intégral de cette Politique est disponible sur le site du CHUQ à l'adresse suivante : [www.chuq.qc.ca](http://www.chuq.qc.ca) sous la rubrique *Politiques*.

Tout membre du personnel des fournisseurs de services informatiques, ou des tiers, responsable de la gestion du matériel informatique, des réseaux d'informations ou d'un système informatique, ou encore d'une partie de celui-ci, a des obligations envers les utilisateurs des systèmes d'informations du CHUQ.

En particulier, la personne:

- prend connaissance de la *Politique en matière de sécurité informationnelle* à l'adresse suivante : [www.chuq.qc.ca](http://www.chuq.qc.ca) et y adhère;
- administre le matériel informatique, le réseau informatique ou les systèmes d'informations de manière licite et efficace;
- respecte le caractère confidentiel de l'information emmagasinée par les utilisateurs ou leur appartenant en propre lors de toute intervention de gestion;
- respecte le caractère confidentiel des renseignements contenus dans des documents auxquels elle aurait pu avoir accès même par mégarde;
- prend des mesures adéquates afin que les utilisateurs puissent travailler dans un environnement garantissant la sécurité et la confidentialité des informations;
- informe les utilisateurs des conventions d'usage et de protection des informations concernant le matériel informatique ou le réseau informatique ou un système informatique ;
- prévient la modification, la corruption et la reproduction illicite des informations, des programmes et des logiciels (incluant la documentation) sous sa responsabilité;
- prend des mesures raisonnables afin d'améliorer, en fonction des besoins, la sécurité des actifs informationnels et de télécommunications, notamment par l'installation des correctifs ou améliorations fournis par les producteurs de logiciels ou par les manufacturiers d'équipements dont il assure le service;
- respecte la confidentialité des connaissances, partielles ou totales, de la structure des réseaux d'information du CHUQ et ne peut divulguer, en tout ou en partie, cette information. De plus, le personnel des fournisseurs de services ou des tiers, doit s'assurer que leur utilisation des réseaux d'informations n'altère pas la structure de ceux-ci;
- s'assure que les personnes non autorisées sous sa responsabilité n'aient pas accès au matériel informatique, aux réseaux d'informations, à un système informatique et aux lieux dont l'accès leur est interdit;
- obtient l'autorisation de l'officier de sécurité informationnelle du CHUQ avant de procéder à un test de sécurité ou à tout autre test pouvant influencer le bon fonctionnement des applications ou des réseaux d'informations;

## **Annexe V - Code de conduite du personnel des fournisseurs de services ou d'un tiers (suite)**

---

- s'engage à ne pas modifier les systèmes d'informations ou installer un actif informationnel sans autorisation préalable des personnes responsables désignées;
- utilise des données fictives ou dénominalisées lors de la formation des utilisateurs, de démonstrations de systèmes ou encore pour les tests requis;
- informe l'officier de sécurité informationnelle du CHUQ de tout manquement à la *Politique en matière de sécurité informationnelle* du CHUQ et au présent code de conduite, et collabore aux suites à donner;
- rend accessible aux utilisateurs, dans des délais raisonnables, le matériel informatique ou les réseaux d'informations dont ils ont besoin dans l'exercice de leurs fonctions;
- respecte la confidentialité des connaissances, partielles ou totales, de la structure des réseaux d'information du CHUQ et ne peut divulguer, en tout ou en partie, cette information. S'assure, de plus, que leur utilisation des réseaux d'informations n'altère pas la structure de ceux-ci;
- respecte l'interdiction d'utiliser des technologies sans fils, ordinateurs de poches ou tout autre type d'équipements de type point d'accès, *Pocket PC<sup>MC</sup>*, *Palm Pilot* ou de tout autre technologie qui pourrait être disponible sans entente préalable avec l'officier de sécurité informationnelle ou d'une personne déléguée par celui-ci, le tout selon des modalités précises;
- assume la responsabilité, donc l'imputabilité des manquements possibles à la présente politique par son rôle et à son niveau de responsabilités.

## Annexe VI - Code de conduite des utilisateurs d'ordinateurs portatifs

---

### Préambule :

Le présent code de conduite a été conçu dans le but de faciliter l'application de la *Politique en matière de sécurité informationnelle* du CHUQ (ci-après désignée Politique). Il doit être respecté et appliqué par tous les membres du personnel du CHUQ qui utilisent ou qui gèrent des renseignements confidentiels et des actifs informationnels ou de télécommunication et par tous les tiers qui ont accès aux actifs informationnels du CHUQ tel que défini dans la présente politique. Le texte intégral de cette politique est disponible sur le site du CHUQ à l'adresse suivante : [www.chuq.qc.ca](http://www.chuq.qc.ca) sous la rubrique *Politiques* et sur l'intranet du CHUQ sous la rubrique DFSIG/SSIG/Sécurité informatique/

### Personnes visées :

Le présent code de conduite s'adresse à tout requérant de privilèges d'utilisation d'un ordinateur portable. Ce code de conduite est réalisé à partir d'extraits de la Politique du CHUQ mentionnée précédemment. Le code de conduite des utilisateurs s'applique également.

### Mises en garde :

Le CHUQ utilise des logiciels permettant de contrôler et d'enregistrer toute utilisation d'Internet faite à partir de ses réseaux d'information. L'officier de sécurité informationnelle du CHUQ se réserve le droit d'enregistrer, peu importe l'utilisateur, toute page World Wide Web (www) visitée, tout « chat » ou « newsgroup » ou courrier électronique.

Le CHUQ analyse et évalue l'usage qui est fait d'Internet, de ses réseaux d'information et du RTSS<sup>MO</sup>. L'usage d'Internet, du RTSS<sup>MO</sup>, des réseaux d'informations et des actifs informationnels et de télécommunications du CHUQ pour des activités illégales entraîne des mesures administratives et disciplinaires. De plus, le CHUQ s'engage à coopérer face à toute requête provenant des forces de l'ordre ou à la demande de tout autre organisme mandaté à cet effet.

### Obligations :

Le requérant de privilèges d'utilisation d'un ordinateur portable s'engage à prendre connaissance de ladite politique, et ce, dès l'obtention de son privilège d'accès et à en respecter les règles et normes.

Dans l'éventualité où l'ordinateur portable est équipé de périphériques intégrés ou externes, incluant particulièrement les graveurs, les lecteurs de disques compacts (CD) et de vidéo numérique (DVD), le requérant s'engage à utiliser ceux-ci selon les normes de sécurité du CHUQ en ce qui a trait à la protection des données et des renseignements confidentiels. Par conséquent les données gravées devront être sous son contrôle, c'est-à-dire conservées en lieu sûr et sous sa responsabilité. Dans le cas d'un projet de recherche, les données devront obligatoirement être dénominalisées avant toute utilisation. Le requérant s'engage, de la même manière, en utilisant un lecteur de disques compacts contenant des données et des renseignements confidentiels à en assurer l'intégrité et la confidentialité.

En tant que personne visée, le requérant s'engage à respecter le Code de conduite des utilisateurs d'ordinateurs portatifs lequel stipule que l'ordinateur portable est un outil mis à la disposition du personnel du CHUQ pour une utilisation professionnelle, plus spécifiquement pour des tâches reliées à l'exercice des fonctions de celui-ci. La Politique mentionnée préalablement, ainsi que le Code de conduite des utilisateurs d'ordinateurs portatifs, émet des règles dans le but que chacun utilise cet accès avec vigilance en respectant entre autres, les droits d'auteur, la propriété intellectuelle, les règles de licences de logiciels, les droits de propriété et la confidentialité des informations et des données.

## **Annexe VI- Code de conduite des utilisateurs d'ordinateurs portatifs** (suite)

---

### **Sanctions prévues :**

Outre l'engagement mentionné au formulaire, tout membre du personnel qui contrevient au code de conduite, à la politique mentionnée et à la réglementation qui en découle est passible des sanctions suivantes, notamment :

- ▶ mesures administratives et disciplinaires ou autres sanctions appropriées à l'intention du personnel conformément aux lois et règlements en vigueur et aux conventions collectives de travail;
- ▶ révocation de certains privilèges d'accès aux équipements et services visés par la présente politique;
- ▶ remboursement au CHUQ de toute somme, y compris les sommes émanant d'un jugement prononcé par tout tribunal ou organisme réglementaire quelconque à l'endroit du CHUQ et qui découlerait de l'utilisation non autorisée, frauduleuse ou illicite de ses services ou de ses actifs informationnels et de télécommunications ou de ses systèmes d'informations.

De plus, le requérant s'engage à rembourser les frais de réparations ou autres frais encourus par le CHUQ et qui seraient reliés à une utilisation non autorisée, inadéquate ou malveillante dudit équipement selon le tarif horaire applicable.

### **Responsabilités de l'utilisateur**

#### ***Tout utilisateur:***

- doit utiliser les actifs informationnels selon les normes permises;
- ne doit utiliser que les codes d'utilisateur ainsi que les mots de passe pour lesquels il a obtenu une autorisation d'usage;
- est responsable des activités résultant de l'usage de ses codes d'utilisateurs ainsi que de ses mots de passe;
- doit prendre des mesures raisonnables afin de protéger ses codes d'utilisateurs, ses mots de passe ainsi que l'intégrité et la confidentialité des actifs informationnels utilisés;
- doit s'abstenir d'utiliser les systèmes d'informations ou de télécommunication à des fins non autorisées, syndicales, commerciales ou illégales;
- ne peut, sans autorisation des personnes concernées, accéder, modifier, reproduire, détruire ou lire des informations, des programmes ou des logiciels;
- doit respecter le caractère confidentiel des données sociosanitaires nominatives, ou des documents, auxquelles il a accès lors de l'exercice de ses fonctions ;
- doit respecter le droit d'auteur des logiciels, des informations et de la documentation utilisés;
- doit s'assurer que tout document à caractère confidentiel, quel que soit son support, soit hors d'atteinte en les rangeant en lieu sûr;
- doit s'assurer que son poste informatique s'il travaille sur les réseaux d'informations reste ouvert la nuit pour le passage de l'antivirus ou s'il travaille sur un poste local, que son logiciel antivirus soit fonctionnel;
- doit voir au respect des règles de sécurité par toute personne de l'extérieur qui vient dans les locaux à titre de visiteur;

## Annexe VI- Code de conduite des utilisateurs d'ordinateurs portatifs (suite)

---

- possédant de l'information concernant tout mécanisme pour détourner ou contrer les systèmes de sécurité mis en place au CHUQ doit en avertir son supérieur immédiat et ne pas utiliser ou diffuser, ledit mécanisme;
- ne peut utiliser les facilités d'accès à Internet ou le RTSS<sup>MO</sup> pour télécharger ou distribuer des données ou des logiciels piratés ou encore pour propager quelque virus que ce soit sur les réseaux d'information du CHUQ;
- ne peut utiliser les facilités d'accès à Internet ou au RTSSMO, ou tout autre moyen, pour rendre inutilisable ou surcharger quelque ordinateur ou réseau que ce soit ou pour contourner tout système mis en place pour protéger la vie privée ou la sécurité des autres utilisateurs;
- ne peut utiliser un modem sur son poste de travail sans l'approbation de l'officier de sécurité informatique du CHUQ;
- doit planifier toute opération de téléchargements intensifs tels que les transferts de documents de grande taille, de documents vidéos ou sonores ou d'envois massifs de courrier électronique en dehors des heures de travail, soit avant 8 h 30, entre 12 h et 13 h ou après 17 h;
- doit vérifier tout document téléchargé contre les virus avant son exécution. L'utilisateur est responsable du contenu desdits documents;
- ne peut divulguer en tout ou en partie la structure des réseaux d'information du CHUQ. De plus, les utilisateurs doivent s'assurer que leur utilisation des réseaux d'information n'altère pas la structure de ceux-ci;
- utilisant les facilités d'accès à Internet doit s'identifier clairement et entièrement quand il participe à des « chats » et à des « newsgroups » ou quand il ouvre un compte sur des systèmes externes;
- doit être autorisé au préalable pour intervenir, au nom du CHUQ, auprès des médias ou à des assemblées publiques. Il peut alors le faire au niveau des clavardages, bavardages en ligne « chats » et des forums de discussions « newsgroups »;
- s'engage à ne pas modifier les systèmes d'informations ou installer un actif informationnel sans autorisation préalable des personnes responsables désignées;
- s'assurer, si l'équipement utilisé lui appartient en propre, de rencontrer les exigences du CHUQ avant de pouvoir communiquer avec les réseaux d'informations mis en place au CHUQ. assumer la responsabilité, donc l'imputabilité des manquements possibles à la présente politique par son rôle et à son niveau de responsabilités.

## Annexe VII- Code de conduite des utilisateurs d'Internet

---

### Préambule :

Le présent code de conduite a été conçu dans le but de faciliter l'application de la *Politique en matière de sécurité informationnelle* du CHUQ (ci-après désignée *Politique*). Il doit être respecté et appliqué par tous les membres du personnel du CHUQ qui utilisent ou qui gèrent des renseignements confidentiels et des actifs informationnels ou de télécommunication et par tous les tiers qui ont accès aux actifs informationnels du CHUQ tel que défini dans la présente politique. Le texte intégral de cette politique est disponible sur le site du CHUQ à l'adresse suivante : [www.chuq.qc.ca](http://www.chuq.qc.ca) sous la rubrique *Politiques*. Le texte intégral de cette politique est disponible sur le site du CHUQ à l'adresse suivante : [www.chuq.qc.ca](http://www.chuq.qc.ca) sous la rubrique *Politiques*.

### Personnes visées :

Le présent code de conduite s'adresse à tout requérant d'un privilège d'accès à Internet. Ce code de conduite est réalisé à partir d'extraits de la politique du CHUQ mentionnée précédemment. Le code de conduite des utilisateurs s'applique également.

### Mises en garde :

Le CHUQ utilise des logiciels permettant de contrôler et d'enregistrer toute utilisation d'Internet faite à partir de ses réseaux d'information. L'officier de sécurité informationnelle du CHUQ se réserve le droit d'enregistrer, peu importe l'utilisateur, toute page World Wide Web (www) visitée, tout clavardage, bavardage en ligne « chat » ou forum de discussions « *newsgroups* » ou courrier électronique.

Le CHUQ analyse et évalue l'usage qui est fait d'Internet, de ses réseaux d'information et du RTSS<sup>MO</sup>. L'usage d'Internet, du RTSS<sup>MO</sup>, des réseaux d'informations et des actifs informationnels et de télécommunication du CHUQ pour des activités illégales ou non autorisées entraîne des mesures administratives et disciplinaires. De plus, le CHUQ s'engage à coopérer face à toute requête provenant des forces de l'ordre ou à la demande de tout autre organisme mandaté à cet effet.

### Obligations :

Le requérant d'un privilège d'accès s'engage à prendre connaissance de ladite politique, et ce, dès l'obtention de son privilège d'accès à Internet et à en respecter les règles et normes.

En tant que personne visée, le requérant s'engage à respecter le Code de conduite des utilisateurs d'Internet, lequel stipule que Internet est un outil mis à la disposition du personnel du CHUQ pour une utilisation professionnelle, plus spécifiquement pour des tâches reliées à l'exercice des fonctions de celui-ci. La politique mentionnée préalablement, ainsi que le code de conduite des utilisateurs d'Internet, émet des règles dans le but que chacun utilise cet accès avec vigilance en respectant entre autres, les droits d'auteur, la propriété intellectuelle, les règles de licences de logiciels, les droits de propriété et la confidentialité des informations et des données.

### Sanctions prévues :

Tout utilisateur qui contrevient au code de conduite, à la politique mentionnée et à la réglementation qui en découle est passible des sanctions suivantes, notamment :

- mesures administratives et disciplinaires ou autres sanctions appropriées à l'intention du personnel conformément aux lois et règlements en vigueur et aux conventions collectives de travail;
- révocation de certains privilèges d'accès aux équipements et services visés par la présente politique;
- remboursement au CHUQ de toute somme, y compris les sommes émanant d'un jugement prononcé par tout tribunal ou organisme réglementaire quelconque à l'endroit du CHUQ et qui découlerait de l'utilisation non autorisée, frauduleuse ou illicite de ses services ou de ses actifs informationnels et de télécommunications ou de ses systèmes d'informations.

## Annexe VII - Code de conduite des utilisateurs d'Internet (suite)

---

### Entre autres, l'utilisateur :

- ▶ doit utiliser les actifs informationnels selon les normes permises;
- ▶ ne doit utiliser que les codes d'utilisateur ainsi que les mots de passe pour lesquels il a obtenu une autorisation d'usage;
- ▶ est responsable des activités résultant de l'usage de ses codes d'utilisateurs ainsi que de ses mots de passe;
- ▶ doit prendre des mesures raisonnables afin de protéger ses codes d'utilisateurs, ses mots de passe ainsi que l'intégrité et la confidentialité des actifs informationnels utilisés;
- ▶ doit s'abstenir d'utiliser les systèmes d'informations ou de télécommunication à des fins non autorisées, syndicales, commerciales ou illégales;
- ▶ doit respecter le droit d'auteur des logiciels, des informations et de la documentation utilisés;
- ▶ doit s'assurer que son poste informatique, s'il travaille sur le réseau, reste ouvert la nuit pour le passage de l'antivirus ou, s'il travaille sur un poste local que son logiciel antivirus est fonctionne;
- ▶ ne peut utiliser les facilités d'accès à Internet ou le RTSS<sup>MO</sup> pour télécharger ou distribuer des données ou des logiciels piratés ou encore pour propager quelque virus que ce soit sur les réseaux d'informations du CHUQ;
- ▶ ne peut utiliser les facilités d'accès à Internet ou au RTSS<sup>MO</sup>, ou tout autre moyen, pour rendre inutilisable ou surcharger quelque ordinateur ou réseau que ce soit ou pour contourner tout système mis en place pour protéger la vie privée ou la sécurité des autres utilisateurs;
- ▶ ne peut utiliser un modem sur son poste de travail sans l'approbation de l'officier de sécurité informatique du CHUQ;
- ▶ doit planifier toute opération de téléchargements intensifs tels que les transferts de documents de grande taille, de documents vidéos ou sonores ou d'envois massifs de courrier électronique en dehors des heures de travail, soit avant 8 h 30, entre 12 h et 13 h ou après 17 h;
- ▶ doit vérifier tout document téléchargé contre les virus avant son exécution. L'utilisateur est responsable du contenu desdits documents;
- ▶ utilisant les facilités d'accès à Internet doit s'identifier clairement et entièrement quand il participe à des clavardages, bavardages en ligne « chats » et à des groupes de discussions « newsgroups » ou quand il sollicite un service auprès des systèmes externes;
- ▶ doit être autorisé au préalable pour intervenir, au nom du CHUQ, auprès des médias ou à des assemblées publiques. Il peut alors le faire au niveau des clavardages, bavardages en ligne « chats » et à des groupes de discussions « newsgroups » ;
- ▶ doit respecter les conventions d'accès et d'usage des réseaux internes et externes, et identifier correctement sa correspondance électronique;
- ▶ doit éviter d'utiliser les facilités d'accès à Internet pour commettre des infractions telles un usage abusif des actifs informationnels et de télécommunications, du harcèlement sexuel, la tenue d'un discours public non autorisé et le détournement ou le vol de la propriété intellectuelle;
- ▶ doit éviter l'affichage de tout document ou tout graphique sexuellement explicite, haineux, raciste ou considéré inacceptable. De tels documents ne doivent pas être archivés, enregistrés, distribués ou édités par les réseaux d'informations du CHUQ;
- ▶ doit éviter tout comportement déviant, usage abusif des systèmes d'informations ou tout comportement nocif ou malveillant tels que les suivants, cités à titre d'exemples:
  - intrusion ou tentative d'intrusion non autorisée dans un poste de travail, dans un système ou dans un réseau interne ou externe;
  - usage volontaire de programmes ou autres moyens qui endommagent les actifs informatiques ou de télécommunication ou leur contenu (ex. : virus informatiques);
  - usage de programmes, de logiciels ou autres moyens en vue d'intercepter, de collecter, de prendre connaissance, de décrypter ou de décoder de l'information (ex. : code d'utilisateur, clé d'accès, fichier ou mots de passe) véhiculée sur un réseau ou résidant sur un poste de travail;
  - utilisation des systèmes d'informations, du courrier électronique ou de la messagerie vocale pour véhiculer des messages ou des propos obscènes, haineux, racistes, diffamatoires, harcelants ou pour commettre tout autre acte réprimé par la loi ou par les règlements du CHUQ;
  - lecture, modification, destruction ou diffusion non autorisée d'informations, de programmes ou de logiciels appartenant à un tiers;
  - interférence volontaire en vue de dégrader la performance d'un poste de travail, d'un système ou d'un réseau informatique;
  - utilisation sans autorisation du code de l'utilisateur ou du code d'accès ainsi que du mot de passe d'un tiers;
  - usage du courrier électronique pour participer à une chaîne de lettres, pour effectuer de la publicité ou de la vente pyramidale ou encore pour faire des envois massifs de messages sans autorisation ou à des fins personnelles;
  - usage déviant ou abusif des systèmes d'informations;
- ▶ assume la responsabilité, donc l'imputabilité, des manquements possibles à la Politique par son rôle et à son niveau de responsabilités.

## RÉFÉRENCES

---

Les références à la base de la présente politique sont les suivantes :

- **QUÉBEC**, Charte des droits et libertés de la personne (L.R.Q c. C-12).
- **CHUQ**, Rapport à la communauté, Québec, 2001-2002,
- **QUÉBEC**, Loi sur la protection de la jeunesse (L.R.Q., c. P-34.1)
- **QUÉBEC**, Loi sur les laboratoires médicaux, la conservation des organes, des tissus, des gamètes et des embryons, les services ambulanciers et la disposition des cadavres. (LRQ, L-0.2)
- **QUÉBEC**, Loi sur les services de santé et des services sociaux (L.R.Q., c.A-4.2).
- **QUÉBEC**, Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c.A-2.1).
- **QUÉBEC**, Loi sur les archives (L.R.Q., c. A-21.1)
- **QUÉBEC**, Loi concernant le cadre juridique des technologies de l'information, (L.R.Q., *chp. C-1.1*)
- **COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC**, Exigences minimales relatives à la sécurité des dossiers informatisés des usagers du réseau de la santé et des services sociaux, Québec, 1992.
- **COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC**, Le courrier électronique, Québec, 1997.
- **MINISTÈRE DE LA SANTÉ ET DES SERVICES SOCIAUX**, Cadre global de gestion des actifs informationnels appartenant aux organismes du réseau de la santé et des services sociaux – Volet sur la sécurité. Québec, 2002.
- **OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE**, Grand dictionnaire terminologique [www.granddictionnaire.com/btml/fra/r\\_motclef/index800\\_1.asp](http://www.granddictionnaire.com/btml/fra/r_motclef/index800_1.asp).
- **UNIVERSITÉ LAVAL**, Politique de sécurité sur les technologies de l'information et des télécommunications, Québec, modifiée en juin 1998.
- **UNIVERSITÉ LAVAL**, Code de conduite sur l'utilisation et la gestion des technologies de l'information et des télécommunications à l'Université Laval, Québec, modifiée en juin 1998.
- **CANADA**, Code criminel.

## DÉFINITIONS DES TERMES

Dans ce document on entend par :

**Actif informationnel et de télécommunication** : banque d'information électronique, système d'information, réseau de télécommunication, technologie de l'information, installation ou ensemble de ces éléments; un équipement médical spécialisé ou ultraspécialisé peut comporter des composantes qui font partie des actifs informationnels, notamment lorsqu'il est relié de façon électronique à des actifs informationnels. S'ajoutent dans le présent document, les documents imprimés par les technologies de l'information

**Audit** : évaluation périodique basée sur des critères définis permettant de vérifier si les normes en vigueur sont appliquées.

**Authentification** : fonction de contrôle de l'accès aux actifs informationnels permettant d'établir la validité de l'identité d'une personne, d'un dispositif ou d'une autre entité au sein d'un système d'information ou de communication.

**Bavardage, bavardage en ligne, Cyberbavardage, Bavardage-Clavier ou Clavardage (Chat)** : conversation écrite, interactive et en temps réel entre des internautes du monde entier, et ceci, par clavier interposé.

**Codes de conduite** : condensés de règles de pratique élaborées à partir de principes moraux et professionnels, devoirs et responsabilités, destiné à établir des règles de conduite à suivre et régissant particulièrement l'utilisation des actifs informationnels et de télécommunications ainsi que la protection des données et des renseignements confidentiels.

**Confidentialité** : propriété que possède une donnée ou une information dont la divulgation, la prise de connaissance et l'utilisation sont réservées à des personnes désignées et autorisées conformément à la présente politique, ses annexes et codes de conduite ainsi que les lois pertinentes en vigueur au Québec.

**Courrier électronique, (courriel) (E-Mail)** : service de correspondance sous forme d'échange de messages, à travers un réseau de téléinformatique. © Commission d'accès à l'information, 1999.

**Disponibilité** : propriété qu'ont les données, l'information et les systèmes d'information et de communication d'être accessibles et utilisables en temps voulu et de la manière adéquate par une personne autorisée.

**Document** : informations portées par un support dont l'information est structurée, de façon tangible ou logique, selon le support qui la porte et intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris des symboles transcritibles sous l'une de ces formes ou un autre systèmes de symboles. Toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite constitue un document. Un dossier peut être constitué d'un ou de plusieurs documents.

**Données sociosanitaires nominatives**: données à caractère confidentiel, qui concernent une personne physique et qui permettent de l'identifier, emmagasinées par un organisme [ou un établissement du réseau] de la santé et des services sociaux.

**Droit d'auteur** : droit exclusif que détient un auteur ou son représentant d'exploiter une œuvre pendant une durée déterminée.

## DÉFINITIONS DES TERMES (suite)

**Engagement de confidentialité** : entente écrite par laquelle le personnel s'engage à respecter toute politique relative à la confidentialité et aux codes de conduite qui en découlent.

**Équipement informatique « hardware »** : ensemble de toutes les composantes physiques incluant les logiciels pour les faire fonctionner et tous les types des périphériques qui forment un système informatique.

**Extrant** : tout objet permettant de conserver de l'information résultant d'un traitement ou des programmes informatiques provenant d'un matériel informatique ou de ses unités périphériques ou d'un équipement de télécommunication.

**Forum, forum de discussion, groupe de discussion (newgroups)** : service offert par un serveur d'information ou un babillard électronique sur un réseau comme Internet et qui permet à un groupe de personnes d'échanger leurs opinions, leurs idées sur un sujet particulier, en direct ou en différé, selon des formules variées (liste de participants, canal IRC, etc.).

**Fournisseur de services** : corporation, société, coopérative ou personne physique faisant affaire, et en mesure de contracter avec le CHUQ, ses unités administratives ou toute autre entité de celui-ci, de ses mandataires ou fiduciaires, qui fournit des services ou des biens à un détenteur, à un utilisateur, à un autre fournisseur, que ce soit en matière de services informatiques ou de tous autres services.

**Gestionnaire de système** : tout membre du personnel dont la fonction est d'assurer la responsabilité de gestion d'actifs informationnels, d'équipements, de systèmes ou de réseaux au sens de la présente politique, et toute personne à qui cette responsabilité est conférée en vertu d'une entente avec le CHUQ.

**Incident** : évènement ayant pu mettre ou ayant mis en péril la sécurité d'un ou de plusieurs actifs informationnels.

**Information** : élément de connaissance susceptible d'être représenté à l'aide de conventions, pour être conservé, traité ou communiqué. (CMTI et AFNOR). ou encore : élément de connaissance descriptif d'une situation ou d'un fait, résultant de la réunion de plusieurs données.

**Intégrité** : propriété d'une information ou d'une technologie de l'information de n'être ni modifiée, ni altérée, ni détruite sans autorisation.

**Internet ou réseau Internet** : réseau informatique mondial constitué d'un ensemble de réseaux nationaux, régionaux et privés, qui sont reliés par le protocole de communication TCP-IP et qui coopèrent dans le but d'offrir une interface unique à leurs utilisateurs.

**Intranet ou réseau intranet** : réseau informatique privé qui utilise des protocoles de communication et des technologies permettant un échange d'information. Les protocoles et les technologies les plus connus sont ceux d'Internet

**Irrévocabilité** : propriété d'un acte d'être définitif et clairement attribué à la personne qui l'a accompli ou au dispositif avec lequel il a été accompli.

**Logiciel** : ensemble de programmes, des procédures et des règles ainsi que du document associé, nécessaires à la mise en œuvre d'un système de traitement de l'information.

**Matériel** : ensemble des éléments physiques employés pour le traitement de l'information.

**Personnel** : ensemble des ressources humaines, rémunérées ou non, qui assument la mission du CHUQ, incluant les utilisateurs.

## DÉFINITIONS DES TERMES (suite)

**Périphérique** : dispositifs servant en premier lieu à l'entrée et à la sortie de données, de même qu'au stockage des données sur supports externes (voir support de données) qui constituent les « périphériques » d'un ordinateur.

**Privilèges d'accès** : autorisation accordée à une personne définissant l'usage qu'elle peut faire des actifs informationnels et de télécommunications.

**Programme** : série de fonctions et de définitions en langage machine ou dans un langage de programmation plus évolué. Elles permettent à l'ordinateur de procéder au traitement des données. On donne aussi aux programmes le nom collectif de logiciel.

**Renseignement** : synonyme d'information.

**Renseignements confidentiels** : tout renseignement personnel qui ne peut être communiqué ou rendu accessible qu'aux personnes ou autres entités autorisées.

**Renseignements personnels ou renseignements nominatifs** : tout renseignement qui concerne une personne physique et qui permet de l'identifier. Sont nominatifs les renseignements qui concernent une personne physique et permettent de l'identifier. Le nom d'une personne physique n'est pas un renseignement nominatif, sauf lorsqu'il est mentionné avec un autre renseignement la concernant ou lorsque sa seule mention révélerait un renseignement nominatif concernant cette personne.

**Réseaux d'informations (syn. réseaux informatiques)** : ensemble des composantes et des équipements informatiques reliés par voie de télécommunications, soit pour accéder à des ressources ou à des services informatisés, soit pour en partager l'accès.

**Réseau de télécommunications sociosanitaires (RTSS<sup>MO</sup>)** : principal véhicule d'échange d'information entre les établissements du réseau de la santé et des services sociaux.

**Site Web** (syn. : web) : site Internet où sont stockées des données accessibles par le Web. Créer un site Web (...) signifie montrer publiquement ses créations. Le site Web permet de conserver [les données,] les textes, les images et les sons, et de les rendre accessibles à toutes les personnes autorisées qui naviguent sur Internet

**Systèmes d'informations** : ensemble organisé de moyens mis en place pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer de l'information en vue de répondre à un besoin déterminé, y incluant notamment les technologies de l'information et les procédés utilisés pour accomplir ces fonctions.

**Technologies de l'information** : tout logiciel ou matériel électronique et toute combinaison de ces éléments utilisés pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'information sous toute forme (textuelle, symbolique, sonore ou visuelle).

**Tiers** : toute personne physique ou morale qui utilise ou accède au nom du CHUQ ou non, à des informations confidentielles ou non, quel que soit le support sur lesquelles elles sont portées.

**Usager** : toute personne qui reçoit des services de santé et des services sociaux.

**Utilisateur** : personne, groupe ou entité administrative faisant usage d'un ou de plusieurs actifs informationnels appartenant au CHUQ ou en faisant partie, incluant les tiers.

### **DÉFINITIONS DES TERMES (suite)**

**Virus** : programme inséré dans un système informatique afin de causer des dommages nuisibles et néfastes.

**Web ou W3** (World Wide Web, WWW): système basé sur l'utilisation de l'hypertexte, qui permet la recherche d'information sur Internet, l'accès à cette information et sa visualisation.