Centre intégré
de santé
et de services sociaux
de la Côte-Nord
Québec

Directive

Utilisation des actifs informationnels

Numéro G1-254-005

1. Objectifs

Le Centre intégré de santé et de services sociaux (CISSS) de la Côte-Nord reconnaît l'importance de donner accès à ses actifs informationnels dont ses équipements et ses ressources informatiques et de télécommunications aux employés et intervenants de l'organisation. Cette utilisation doit être encadrée de façon à répondre aux besoins organisationnels.

Le CISSS de la Côte-Nord fournit à ses employés et à ses intervenants divers outils de travail informatiques visant à les soutenir dans leurs tâches afin qu'ils puissent les accomplir plus aisément et permettre ainsi d'accroître l'efficacité.

En effet, dans leur milieu de travail, les employés et intervenants ont accès à différents systèmes électroniques, notamment des ordinateurs (de table ou portatifs), des téléphones intelligents, des tablettes numériques, des boîtes vocales, des télécopieurs, du courrier électronique de même qu'à Internet.

La présente directive vise à établir les conditions relatives à l'utilisation sécuritaire par les employés et les intervenants du CISSS de la Côte-Nord des équipements, des systèmes, des logiciels et du réseau de même que des données contenues ou véhiculées par eux.

L'utilisation des ressources et systèmes informatiques comporte certains risques pour le CISSS de la Côte-Nord, par exemple voir sa responsabilité engagée pour l'atteinte à des droits d'auteurs, la diffusion de renseignements personnels protégés par la Loi sur la protection des renseignements personnels, la diffusion ou la transmission de messages disgracieux, de mauvais goûts, discriminatoires et/ou illégaux ou encore voir son réseau informatique monopolisé par une surcharge ou infecté par un virus.

Ainsi, il est primordial que les employés et les intervenants utilisent tous les actifs informationnels de façon appropriée, assurent la confidentialité, protègent la vie privée et appliquent les meilleures pratiques en matière de sécurité.

2. Cadre juridique et administratif

La présente directive s'inscrit dans un cadre juridique régissant l'utilisation des technologies de l'information et l'accès à l'information, notamment :

- De la *Loi sur les services de santé et les services sociaux* (RLRQ, c. S-4.2);
- De la *Loi concernant le cadre juridique des technologies de l'information* (RLRQ, c. C-1.1);
- De la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1);
- De la *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ, c. P-39.1);
- De la Politique de sécurité de l'information du CISSS de la Côte-Nord G1-252-004;
- De la Politique d'utilisation des médias sociaux du CISSS de la Côte-Nord G1-252-005;

- Du Cadre de gestion de la sécurité de l'information du CISSS de la Côte-Nord;
- De la Règle particulière sur la sécurité organisationnelle du MSSS (2013).

3. Champ d'application

La présente directive s'applique à tous les utilisateurs des actifs informationnels appartenant au CISSS de la Côte-Nord ou sous sa responsabilité, notamment tout employé, médecin, résident, chercheur, membre du conseil d'administration, stagiaire, étudiant, consultant ou bénévole, ci-après désigné « utilisateurs ».

La directive porte sur l'utilisation des actifs informationnels appartenant au CISSS de la Côte-Nord ou placés sous sa responsabilité que sont :

- Le réseau informatique et de télécommunications du CISSS de la Côte-Nord;
- Les équipements informatiques et de télécommunications appartenant au CISSS de la Côte-Nord;
- Les équipements informatiques et de télécommunications qui n'appartiennent pas au CISSS de la Côte-Nord, mais qui sont en lien avec son réseau, incluant les appareils intelligents sans fil;
- Les logiciels et les données qui résident ou qui transitent sur le réseau du CISSS Côte-Nord et les données qui y sont associées;
- Tous les documents numériques détenus et hébergés par le CISSS de la Côte-Nord peu importe leur forme et quels que soient les supports sur lesquels ils sont fixés;

On entend par équipements informatiques et de télécommunications les ordinateurs (de table ou portatifs), les téléphones intelligents, les tablettes numériques, les boîtes vocales, les télécopieurs, les imprimantes multifonctions ainsi que tout autre système électronique ou périphérique informatique mis à la disposition des utilisateurs.

4. Définitions

Actif informationnel : une banque d'information, un système d'information, un réseau de télécommunications, une infrastructure technologique ou un ensemble de ces éléments ainsi qu'une composante informatique d'un équipement médical spécialisé ou ultra spécialisé. Est également considéré comme un actif informationnel, tout support papier contenant de l'information.

Réseau : Tout réseau de communication accessible par l'intermédiaire des équipements et des ressources informatiques et de télécommunications, contrôlé ou administré par le CISSS de la Côte-Nord.

5. Propriété des systèmes électroniques

Les équipements informatiques et de télécommunications, les droits d'utilisation des logiciels, les connexions Internet, les comptes de courriel ainsi que toutes les informations emmagasinées par les systèmes d'information, pour lesquels les droits d'usage ont été acquittés ou sont détenus par le CISSS de la Côte-Nord demeurent la propriété exclusive du CISSS de la Côte-Nord.

Des systèmes d'information, notamment des services de courriel, d'Internet et de différents outils collaboratifs sont également partagés ou offerts par le CISSS de la Côte-Nord. Ceux-ci peuvent être soumis à des règles et des exigences particulières de l'établissement.

Toute information qui est créée, envoyée, reçue, mémorisée et généralement conservée par les systèmes d'information du CISSS de la Côte-Nord fait partie intégrante des registres du CISSS de la Côte-Nord et, par le fait même, est sa propriété exclusive. Conséquemment, l'expectative de vie privée des utilisateurs est limitée lors de l'utilisation des technologies de l'information, de l'Internet et du courrier électronique.

6. Utilisation à des fins organisationnelles

Les équipements et systèmes d'information sont mis à la disposition des utilisateurs du CISSS de la Côte-Nord aux fins de leur travail afin de soutenir les différentes tâches qu'ils doivent accomplir et, du même coup, accroître leur efficacité. Ces équipements et systèmes d'information ne doivent pas être utilisés à des fins personnelles.

Une utilisation personnelle peut être admise, **à titre exceptionnel**, par le supérieur immédiat, dans la mesure où elle ne constitue pas un abus, notamment qu'elle ne surcharge pas l'infrastructure informatique (stockage ou transfert de fichiers, connexion à des sites radiophoniques ou utilisation de messageries instantanées, par exemple : CHAT), ne contrevient pas aux règles énoncées dans cette directive et ne vise aucun but lucratif.

7. Conditions d'utilisation des actifs informationnels

7.1 Utilisation responsable

Seuls les utilisateurs dûment autorisés peuvent avoir accès aux actifs informationnels du CISSS de la Côte-Nord, selon leurs fonctions et dans les limites de l'autorisation qui leur a été accordée. L'utilisation de ces actifs informationnels doit être faite de façon pertinente, raisonnable et efficace.

Le CISSS de la Côte-Nord peut aviser la personne concernée que son usage des actifs informationnels est irrégulier et voir à ce que la situation soit corrigée.

7.2 Protection de l'identifiant et des codes d'accès

Les utilisateurs doivent en tout temps assurer l'intégrité, la confidentialité des informations, qu'elles soient de nature administrative ou clinique, échangées au moyen des équipements et systèmes d'information. Ainsi, il est de la responsabilité des utilisateurs d'utiliser les moyens appropriés pour communiquer, échanger ou recevoir des informations confidentielles. À ces fins, les codes d'accès, les mots de passe et les autorisations qui ont été octroyés ne doivent en aucun cas être partagés.

L'utilisateur est tenu en tout temps de préserver la confidentialité du mot de passe associé à un identifiant qui lui a été attribué (ex. : un code d'accès). Dans le cas d'un identifiant matériel (ex. : clé, carte magnétique, etc.), la personne concernée doit en protéger l'accès et l'utilisation.

L'utilisateur est responsable de l'exactitude de ses données d'identité qui doivent être valides et complètes en tout temps. En cas d'inexactitude, l'utilisateur doit les faire rectifier rapidement auprès de la Direction des ressources humaines, communications et affaires juridiques (DRHCAJ).

Un utilisateur est réputé responsable des activités effectuées avec son identifiant et le mot de passe qui y est associé. La personne informée que le mot de passe qui protège cet identifiant a été compromis doit le changer dans les plus brefs délais et en aviser le Centre de services (CS).

Un utilisateur ne peut atténuer, contourner ou modifier le contrôle d'accès et le fonctionnement d'un actif informationnel appartenant au CISSS de la Côte-Nord ou sous la responsabilité de celui-ci.

7.3 Protection de l'information

Les communications peuvent facilement être interceptées sur le réseau Internet et toutes les informations confidentielles appartenant au CISSS de la Côte-Nord ou qui lui ont été confiées ne doivent donc pas être transmises par Internet, par courrier électronique ou par un autre moyen de communication électronique à moins que les messages n'aient d'abord été cryptés et signés en utilisant la méthode autorisée par le CS. Le destinataire devra communiquer avec l'émetteur pour obtenir une copie.

Dans le cas de l'utilisation des appareils mobiles, les utilisateurs ne doivent pas utiliser la fonction photo des téléphones intelligents pour conserver, échanger ou acheminer des données cliniques ou nominatives. Les informations ainsi collectées ou échangées ne bénéficient d'aucune protection et peuvent être interceptées ou utilisées à d'autres fins.

Les médias amovibles, comme les clés USB, sont également des sources importantes de fuites d'information. Il est recommandé de ne jamais copier d'informations sensibles ou confidentielles sur ces médias. Si des informations sensibles doivent tout de même être copiées sur ces médias, il existe des clés USB cryptées et protégées. De même, toute copie de données confidentielles ou sensibles sur CD, DVD ou autre média doit être protégée par chiffrement. Il est de la responsabilité de l'utilisateur de faire preuve de vigilance lors de l'utilisation de ces médias.

7.4 Protection des équipements

L'utilisateur des actifs informationnels du CISSS de la Côte-Nord doit veiller à ce que l'équipement informatique utilisé ou placé sous sa responsabilité soit employé de façon adéquate afin d'assurer son intégrité (par exemple : protection contre les virus et autres logiciels malveillants, utilisation par les personnes autorisées seulement). Lorsqu'il lui semble que la sécurité de ces actifs est compromise ou pourrait être compromise, l'utilisateur doit le signaler au CS.

Les équipements informatiques ou de télécommunications peuvent faire l'objet de perte ou de vol. L'utilisateur ou la personne responsable de l'équipement du CISSS de la Côte-Nord doit garantir la protection physique de ces équipements en mettant en place des mesures appropriées, avec le soutien du CS.

7.5 Utilisation de réseaux sans fil publics

Les réseaux sans fil publics font souvent l'objet de piratage. Les utilisateurs doivent s'assurer d'utiliser des réseaux sans fil sécuritaires, notamment les réseaux domestiques ou organisationnels comme ceux d'autres organisations gouvernementales.

7.6 Restrictions Internet

Le CISSS de la Côte-Nord effectue le filtrage Web au niveau régional et se réserve le droit d'interdire ou de bloquer l'accès de certains sites Internet dont le contenu est illégal ou non approprié aux fins d'affaires de l'établissement.

Certains sites sont bloqués par le système de filtrage Web provincial du MSSS.

7.7 Respect du droit à l'image

Les lois canadiennes et québécoises encadrent le droit à l'image des citoyens. Ainsi, le fait de photographier ou filmer un individu ou un client sans son consentement explicite constitue une violation du droit à la vie privée.

Afin de préserver la confidentialité et prévenir toute situation qui pourrait nuire à la vie privée des employés et des usagers, il est strictement interdit d'utiliser un appareil de télécommunications pour effectuer des photos, des vidéos, de l'enregistrement audio ou vocal et de faire circuler l'information par texto, toute forme de systèmes d'information tels le CHAT, sauf si une autorisation préalable de l'organisation est obtenue ainsi que le consentement écrit du client.

8. Activités prohibées

L'utilisateur ne peut :

- Utiliser les équipements informatiques et de télécommunications du CISSS de la Côte-Nord (incluant les portables, appareils mobiles et périphériques amovibles) d'une manière qui aurait pour effet de nuire à la réputation du CISSS de la Côte-Nord, par exemple, utiliser un logiciel pirate, utiliser un mot de passe qui n'est pas le sien, tenter d'infiltrer d'autres ordinateurs sur le réseau Internet, visionner ou échanger du matériel pornographique ou obscène, envoyer des messages pouvant être considérés comme étant de la discrimination ou du harcèlement.
- Utiliser les technologies de l'information pour des activités illégales ou malhonnêtes ou pour harceler un autre membre du personnel du CISSS de la Côte-Nord ou toute autre personne.
- Visionner, télécharger, copier, partager ou expédier des images ou des fichiers érotiques, de pornographie juvénile ou de sexualité explicite, ou dont le contenu a un caractère diffamatoire, offensant, harcelant, haineux, violent, menaçant, raciste, sexiste, ou qui contrevient à l'une des dispositions de la Charte des droits et libertés de la personne (L.R.Q., c. C-12), ainsi que de toutes autres lois au Québec.
- Télécharger ou transmettre du matériel breveté ou protégé par les droits d'auteur ou les marques de commerce, des secrets commerciaux, des informations ou des documents illégaux ou autres informations ou documents confidentiels ou privés sans l'autorisation préalable du CISSS de la Côte-Nord.
- Télécharger des émissions de radio ou télévision en continu, des films ou de la musique.
- Partager ou copier un logiciel installé sur l'équipement du CISSS de la Côte-Nord auquel il a accès sans autorisation préalable.

- Utiliser à son profit les équipements informatiques et de télécommunications mises à sa disposition ou pour transmettre de la publicité, faire de la promotion ou d'effectuer des transactions dans le cadre d'un commerce personnel.
- Utiliser, sans autorisation, le code d'utilisateur ou le mot de passe d'un autre ou divulguer quelques codes ou mots de passe, y compris le sien.
- Accéder sans autorisation et à distance à des ordinateurs ou autres systèmes ou endommager, altérer ou perturber ces ordinateurs ou systèmes de quelque façon que ce soit.
- Permettre à un tiers, sans autorisation, d'accéder aux équipements informatiques et de télécommunications ou d'utiliser les systèmes d'informations du CISSS de la Côte-Nord y compris de fournir accès à de l'information confidentielle à des personnes qui n'y ont pas droit ou autrement compromettre la sécurité de ses systèmes électroniques.
- Utiliser les systèmes d'information du CISSS de la Côte-Nord, notamment le courriel, pour des envois massifs de messages pour des fins de sondage, de publicité ou d'événement sans relation avec les activités du CISSS de la Côte-Nord.
- Utiliser Internet et le courrier électronique à des fins personnelles comme les jeux en ligne ou autres activités n'ayant aucun lien avec les activités professionnelles reliées au travail de l'utilisateur.
- Créer, expédier ou réexpédier tout message électronique ou fichier qui contient un élément qui contrevient aux paragraphes qui précèdent.
- Créer, expédier ou réexpédier tout message électronique ou fichier qui est susceptible d'affecter le fonctionnement de l'équipement mis à sa disposition ou le réseau du CISSS de la Côte-Nord auquel il est relié, ou d'engendrer des coûts additionnels à l'employeur.
- Exercer des moyens de pression ou soutenir de tels moyens à des fins de manifestation ou d'incitation à des manifestations.
- Utiliser les fonctions automatiques de réexpédition de courriel, car elles peuvent mener à la divulgation de données confidentielles ou nominatives surtout si le service visé est sur Internet.
- Retransmettre les messages non pertinents au travail (humour, chaîne de lettres, photos, vidéo ou autre) acheminés à un grand nombre d'utilisateurs, car ils créent une forme de pollution dans les courriels et font perdre un temps précieux à plusieurs utilisateurs.
- Diffuser ou publier, sur Internet ou sur tout autre environnement public, de l'information, de quelque nature que ce soit, concernant le CISSS de la Côte-Nord, sauf s'ils y sont spécifiquement autorisés.
- Introduire des virus, tenter de percer les systèmes de sécurité ou procéder à des altérations illicites à l'aide des systèmes électroniques du CISSS de la Côte-Nord.
- Réaliser des modifications de la configuration du navigateur Internet ou utiliser un navigateur Internet non autorisé. Ces interventions sont effectuées par ou sous contrôle du CS.
- Désactiver, détruire ou contourner quelque mesure de sécurité que ce soit, mise en place pour protéger la confidentialité ou la sécurité des équipements informatiques et de télécommunications.

8.1 Vigilance

Compte tenu des menaces informatiques présentes sur Internet et dans les courriels, les utilisateurs doivent faire preuve de vigilance lorsqu'ils reçoivent des courriels non sollicités ou qu'ils naviguent sur Internet.

Les utilisateurs ne doivent pas tenter d'accéder un site au moyen de liens Internet dont l'usage est inconnu ou ouvrir des pièces jointes dont la provenance est inconnue ou douteuse. En cas de doute, les utilisateurs doivent contacter le CS.

9. Journalisation

Pour des fins de sécurité, ou afin de respecter des exigences légales, la plupart des actions sur les équipements et les systèmes d'information sont journalisées. Les utilisateurs ne doivent nullement prendre pour acquis que les informations mémorisées sur les ordinateurs, les disques durs, les courriels ou lors de la navigation sur Internet sont privées. Ainsi, aucun utilisateur ne doit s'attendre à une quelconque intimité relativement à son utilisation des systèmes électroniques.

Les mots de passe et codes d'utilisateur n'ont que pour seule fin d'empêcher les tiers d'avoir accès aux informations confidentielles du CISSS de la Côte-Nord. Ils n'ont pas pour but de protéger la vie privée des utilisateurs.

10. Surveillance des actifs informationnels

Toujours dans un objectif d'assurer la sécurité des systèmes électroniques, des mécanismes de surveillance et de contrôle sont mis en place dans le but d'assurer la protection des équipements informatiques et de télécommunications ainsi que des systèmes d'information, leur bon fonctionnement et le respect de cette directive.

En outre, le CISSS de la Côte-Nord se réserve le droit de faire toute vérification ou enquête sur toute irrégularité, réelle ou présumée, portée à son attention et de dévoiler ces communications à toute autorité officielle ou à toute autre tierce partie.

11. Sanctions

Tout manquement à la présente directive peut mener à l'imposition de mesures disciplinaires, administratives ou légales en fonction de la gravité et des conséquences de son geste, et/ou à l'annulation des privilèges d'accès de l'utilisateur aux actifs informationnels.

Le CISSS de la Côte-Nord se réserve également le droit de tenir un utilisateur personnellement responsable pour tout dommage encouru à l'occasion ou résultant d'une contravention aux règles contenues aux présentes.

12. Signalement d'un incident

Chaque personne œuvrant dans l'établissement est responsable de signaler les cas d'activités interdites, illégales ou malhonnêtes énumérées à l'article 8 de la présente directive dont il pourrait être témoin.

L'utilisateur doit se référer à la directive de la gestion des incidents de sécurité et au processus d'escalade pour connaître la procédure à utiliser ou encore se référer au responsable de la sécurité de l'information de l'établissement.

13. Entrée en vigueur et consultation

Versions	Préparée par	Instances consultées						Entrée en vigueur
		CODIR	CII	CM	CMDP	CA	Autres	
1	Anne Paquet, conseillère en gouvernance de la sécurité de l'information François Otis, chef de service exploitation et infrastructures Michel Rioux, directeur des ressources informationnelles	✓					Comité de sécurité	Le 23 mai 2017
2								
3								

CA	Conseil d'administration	CMDP	Conseil des médecins, dentistes et pharmaciens
CII	Conseil des infirmières et infirmiers	CODIR	Comité de direction
CM	Conseil multidisciplinaire		

14. Références

Directive sur l'utilisation des systèmes électroniques du CIUSSS de l'Estrie – CHUS.
Directive sur l'utilisation éthique des technologies de l'information du CSSS de Chicoutimi.
Directive sur l'utilisation éthique des technologies de l'information MSSS05-005