Directive sur l'utilisation éthique des technologies de l'information

N° d'identification : DIR-SEC-RI.1

Référence à la politique n° : DRI 503 – Sécurité de l'information

CE DOCUMENT S'ADRESSE AUX PERSONNES SUIVANTES :
Cette directive doit être respectée par tous les utilisateurs des technologies de l'information incluant le personnel, les médecins, les résidents, les étudiants, les stagiaires, les contractuels et les fournisseurs ou toute autre personne utilisant les actifs informationnels du CIUSSS. Cette directive s'applique également aux utilisateurs externes du réseau de la santé et des cliniques privées ayant accès aux bases de données de notre établissement.
CE DOCUMENT EST ACCESSIBLE :
☐Répertoire commun ☐Site Internet ☒ Intranet ☐Autre Précisez :

NOMBRE DE PAGES	10
RESPONSABLE DE L'APPLICATION	Direction des ressources informationnelles
RESPONSABLE DE LA CODIFICATION ET DE LA CONSERVATION DU DOCUMENT	
INSTANCE(S) CONSULTÉE(S)	Comité de sécurité des actifs informationnels
RESPONSABLE DE L'ADOPTION OU DE LA RÉVISION FINALE	Comité de sécurité des actifs informationnels
DATE DE LA MISE EN VIGUEUR	2010
DATE DE L'ADOPTION OU DE LA RÉVISION ET NUMÉRO DE RÉSOLUTION DU C.A.	Février 2017 – Révision CIUSSS
RÉVISION	

1. Objectif

Cette directive a comme objectif d'établir le cadre d'utilisation des technologies de l'information, plus particulièrement du réseau Internet et du courrier électronique pour toutes les personnes œuvrant au Centre de santé et de services sociaux (CIUSSS) du Saguenay–Lac-Saint-Jean et les règles générales de conduite et de sécurité auxquelles elles doivent souscrire.

L'utilisation d'Internet et du courrier électronique fera l'objet de procédures spécifiques puisque ces outils sont susceptibles d'avoir des impacts importants sur l'organisation des soins et services à la population, sur la productivité du personnel, sur la performance des infrastructures informatiques et sur la sécurité informationnelle s'ils ne sont pas utilisés conformément aux exigences établies. De plus, la responsabilité légale qui peut lier l'employeur nécessite qu'elles soient utilisées judicieusement et avec éthique.

Cette directive vise à :

- Promouvoir les bonnes pratiques par une utilisation responsable et éthique des ressources informationnelles et en informer les utilisateurs.
- Utiliser judicieusement les biens de l'établissement.
- Assurer un comportement individuel et collectif conforme aux attentes de l'établissement pour permettre de répondre aux exigences de l'établissement et de toute législation et réglementation applicables.
- Contribuer à la réalisation de la mission du CIUSSS en assurant la protection des renseignements personnels, plus précisément leur disponibilité, leur intégrité et leur confidentialité afin de protéger ultimement l'information sur les usagers.
- Préserver la réputation et l'image du CIUSSS.
- Prévenir une utilisation abusive ou illégale des ressources informationnelles de la part des utilisateurs.
- Minimiser les risques de destruction ou de modification des systèmes et données par l'introduction de virus.

2. Contexte

Cette directive découle directement de la politique sur la sécurité de l'information de l'établissement.

Cette directive respecte les exigences du cadre global de gestion sur la sécurité des actifs informationnels du réseau de la santé et des services sociaux et intègre les exigences de la directive de sécurité sur l'utilisation éthique des technologies de l'information du MSSS.

3. Étendue des règles

Ce document établit les règles à respecter au Centre intégré universitaire de santé et services sociaux (CIUSSS) du Saguenay–Lac-Saint-Jean concernant l'utilisation de ses systèmes électroniques, notamment le courrier électronique, les ordinateurs et les autres équipements qui leur sont reliés, le réseau Internet et les dossiers sur support informatique.

4. Règles générales

Tous les systèmes électroniques utilisés dans l'environnement du CIUSSS doivent être autorisés par les instances concernées.

Tous les utilisateurs des systèmes électroniques du CIUSSS acceptent, dans leur utilisation, de respecter les règles qui sont établies dans le présent document.

Le CIUSSS se réserve le droit de modifier ces règles en tout temps.

Internet est un réseau mondial reliant plusieurs millions d'ordinateurs. Il s'agit d'un réseau public orienté sur les facilités d'accès et de communication et sur lequel on retrouve de multiples services particulièrement :

- L'accès par navigation à des millions de sites et de banques de données;
- Le courrier électronique;
- Le transfert de fichiers;
- Le téléchargement de programmes;
- Les groupes de discussion et outils collaboratifs (incluant les médias sociaux).

Le recours à ces technologies, y compris Lotus Notes que nous utilisons comme courrier électronique au sein du MSSS, nous confronte cependant à des problématiques d'éthique qui étaient relativement bien maitrisées dans le cadre de moyens de communication plus traditionnels. Cette directive rappelle les règles qui s'appliquent en regard de l'utilisation de ces technologies et précise la conduite à respecter. L'établissement établit également par cette présente directive les règles d'utilisation éthiques en matière de comportements attendus de la part des utilisateurs et les activités de gestion de ces technologies en termes de droits d'accès et de surveillance de l'utilisation qui en est faite.

Dans ce contexte, voici les clauses que l'utilisateur s'engage à respecter afin de protéger les actifs informationnels de l'établissement.

5. Règles spécifiques

5.1. Propriétés des messages et de l'information

Les informations enregistrées sur les systèmes électroniques du CIUSSS demeurent son entière propriété. Toute information ou tout message qui est créé, envoyé, reçu, enregistré ou auquel on peut avoir accès par les systèmes électroniques fait partie des registres du CIUSSS.

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.

5.2. Utilisation aux fins d'affaires seulement

Les systèmes électroniques du CIUSSS, qui couvrent également l'utilisation du réseau Internet et du courrier électronique, doivent être utilisés uniquement dans le cadre des activités de l'établissement et ne peuvent être utilisés à des fins personnelles.

Une utilisation personnelle est admise à titre exceptionnel, en dehors des heures de travail, 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 : SMS), ne contrevient pas aux règles énoncées dans cette directive et ne vise aucun but lucratif.

5.3. Garantie de confidentialité

Malgré toutes les mesures de sécurité mises en place et l'utilisation de mots de passe :

- En naviguant sur le réseau Internet, les utilisateurs doivent se rappeler qu'il y a une journalisation et qu'il peut y avoir une surveillance, un contrôle et une compilation des sites visités.
- Les utilisateurs doivent se rappeler que les communications qu'ils créent, envoient, reçoivent ou enregistrent sur les systèmes électroniques du CIUSSS pourraient être lues ou entendues par quelqu'un d'autre que le destinataire suite à des actions malveillantes.

5.4. Droit de surveillance du CIUSSS envers ses actifs informationnels

Le CIUSSS ne surveillera pas systématiquement tous ses actifs informationnels et toutes les communications (courriel, accès Internet), mais se réserve le droit de surveiller, accéder, récupérer et lire les communications dans certaines circonstances, comme :

- Lorsqu'il est urgent et légitime pour le CIUSSS de le faire.
- Lorsqu'un rapport d'incident de sécurité est rédigé et que l'enquête exige d'avoir accès à ces messages.
- Lorsqu'un message d'alerte de virus est transmis au responsable de la sécurité de l'information et au service informatique.
- Lors d'audit de sécurité afin de valider le bon fonctionnement des liens de communications et des systèmes d'informations.
- Lorsque le CIUSSS a des motifs raisonnables de croire qu'un utilisateur se comporte ou est sur le point de se comporter de manière inappropriée en relation avec les systèmes électroniques du CIUSSS.
- Lorsque le CIUSSS croit raisonnablement qu'un utilisateur a commis ou est sur le point de commettre un crime ou autre délit qui pourrait nuire directement ou indirectement au CIUSSS.
- Lorsque le CIUSSS doit examiner le contenu des messages pour obtenir de l'information qui n'est pas autrement disponible.
- Lorsqu'il est requis pour le CIUSSS de le faire par la loi ou par une ordonnance de la Cour.
- Lorsque l'utilisateur en question n'est pas disponible pour cause de décès, maladie, vacances ou ne travaille plus pour le CIUSSS.
- Lorsqu'un utilisateur quitte le CIUSSS, celui-ci se réserve le droit de conserver l'adresse électronique de l'utilisateur pendant un délai raisonnable suivant son départ afin de s'assurer que des communications importantes puissent être transmises au CIUSSS.

Cependant, le CIUSSS surveillera systématiquement les fichiers téléchargés et les sites visités afin de s'assurer de l'utilisation appropriée et sécuritaire d'Internet, et ce, pour tous les utilisateurs.

Dans le cadre des activités de surveillance réalisées par un nombre restreint de personnes, le CIUSSS s'engage à protéger la confidentialité des renseignements obtenus par de telles activités. Les personnes pouvant avoir accès à ces informations sont le gestionnaire concerné, les personnes désignées par la DRHCAJ, le RSI (responsable de la sécurité de l'information ou son délégué, le détenteur, les RPRP (responsables de la protection des renseignements personnels) et le PDG (Président directeur général).

5.5. Protection de l'information

Puisque les communications peuvent facilement être interceptées sur le réseau Internet, toutes les informations confidentielles appartenant au CIUSSS ou confiées à ce dernier devraient être cryptées et signées avant d'être transmises par Internet, par courrier électronique ou par un autre moyen de communication électronique.

5.6. Rédaction des messages

L'utilisateur doit rédiger ses messages de courrier électronique avec le plus grand soin. Les messages envoyés par courrier électronique doivent être reliés au travail. Dans le cas de pièces à joindre au courriel, une attention doit donc être apportée au volume des pièces jointes.

Même si un message a été effacé, une copie de sauvegarde existe probablement et il est parfois possible de reconstituer le message. Le message peut également avoir été imprimé ou encore transmis à quelqu'un d'autre sans le consentement de l'auteur du message. L'utilisateur doit exercer toute la prudence voulue en créant des fichiers sur support informatique, lesquels peuvent lier le CIUSSS au même chef que des dossiers physiques.

5.7. Restrictions quant aux sites visités via Internet

L'établissement interdit l'accès aux sites Internet n'ayant pas d'intérêt pour la mission de l'établissement notamment, à tout document pornographique, haineux, raciste ou socialement inacceptable. De plus, de tels documents ne doivent pas être archivés, enregistrés, distribués ou édités sur les réseaux de l'établissement.

Certains sites sont déjà bloqués par le système de filtrage de l'établissement et du MSSS

6. Activités prohibées

L'utilisateur ne peut :

- Présenter, sur les réseaux sociaux, son opinion comme étant celle du CIUSSS.
- Utiliser les systèmes électroniques du CIUSSS (incluant les portables et périphériques amovibles) d'une manière qui aurait pour effet de nuire à la réputation du CIUSSS, par exemple, utiliser un logiciel pirate ou sans droit de licence, 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.

    - Visionner, télécharger en amont ou en aval, accéder, créer, distribuer, copier, partager ou autrement transmettre du matériel sexuellement explicite tel que les images ou vidéos érotiques, pornographie juvénile ou de sexualité explicite.
    - Visionner, télécharger, accéder, créer, distribuer, copier, partager ou autrement transmettre du contenu à 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.
    - Télécharger en amont ou en aval, ou autrement 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 CIUSSS.
    - Partager ou copier un logiciel installé sur l'équipement du CIUSSS auquel il a accès sans autorisation préalable.
    - 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.
    - Utiliser, sans autorisation, le code d'utilisateur ou le mot de passe d'un autre ou divulguer quelques code ou mot de passe, y compris le sien.
    - Permettre à un tiers, sans autorisation, d'accéder ou d'utiliser les systèmes électroniques du CIUSSS, 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.
    - Ouvrir du courrier électronique qui ne lui est pas adressé ou envoyer des messages anonymes par courrier électronique ou par télécopieur.
    - Créer, expédier ou réexpédier tout message électronique ou fichier qui est susceptible d'affecter le fonctionnement de l'équipement mis à sa disposition ou du réseau du CIUSSS auquel il est relié, ou d'engendrer des coûts additionnels à l'employeur.
    - Utiliser les technologies de l'information pour des activités illégales ou malhonnêtes ou pour harceler un autre membre du personnel du CIUSSS ou toute autre personne.
    - Utiliser Internet et le courrier électronique à des fins personnelles telles que les jeux en ligne ou autres activités n'ayant aucun lien avec les activités professionnelles reliées au travail de l'utilisateur.
    - Utiliser à son profit les ressources informationnelles 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.

- Exercer des moyens de pression ou soutenir de tels moyens à des fins de manifestation ou d'incitation à des manifestations.
- Télécharger des émissions de radio ou de télévision en continu, des films ou de la musique.
- 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.
- Introduire des virus, tenter de percer les systèmes de sécurité ou procéder à des altérations illicites à l'aide des systèmes électroniques du CIUSSS.
- 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 service informatique.
- Installer ou utiliser du matériel informatique personnel sur le réseau informatique du CIUSSS sans autorisation préalable.

7. Mesures disciplinaires

Étant donné que l'établissement demeure responsable de l'utilisation faite par les utilisateurs des technologies de l'information lui appartenant, toute personne qui enfreint les dispositions de cette directive s'expose à des mesures disciplinaires, administratives ou légales en fonction de la gravité et des conséquences de son geste.

8. Signalement des activités prohibées

La gestion de la sécurité se fait par plusieurs acteurs dans l'organisation. Chaque personne œuvrant dans l'établissement est donc responsable de signaler les cas d'activités interdites, illégales ou malhonnêtes énumérées à l'article 7 de la présente directive.

9. Responsabilités

9.1. Comité de sécurité des actifs informationnels

- Approuver cette directive.

9.2. Directeur des ressources informationnelles

- S'assurer que le personnel sous sa supervision soit informé de l'existence et du contenu de cette directive et contribue à sa mise en application.

9.3. Responsable de la sécurité de l'information (RSI)

- Maintenir la directive à jour;
- Diffuser les modifications;
- Aider à l'interprétation, lorsque nécessaire;
- S'assurer de l'application de cette direction.

9.4. Conseiller en gouvernance de la sécurité de l'information

- Maintenir la directive à jour;
- Diffuser les modifications;
- Aider à l'interprétation, lorsque nécessaire;
- S'assurer de l'application de cette direction.

9.5. Gestionnaire

- S'assurer que tout le personnel du service est informé de l'existence et du contenu de cette directive.
- Aviser le responsable de la sécurité de l'information ou le directeur des ressources humaines, des communications et des affaires juridiques s'il découvre un utilisateur faisant un usage abusif ou non conforme à la directive.
- Autoriser la demande d'accès aux différents systèmes électroniques et au réseau Internet du personnel de son service.
- Acheminer à la DRI (direction des ressources informationnelles) les demandes d'accès aux différents systèmes électroniques et au réseau Internet qui sont nécessaires à l'accomplissement du travail après en avoir évalué le besoin réel.
- Appliquer les mesures disciplinaires, administratives ou légales en fonction de la gravité et des conséquences du geste posé par l'employé.

9.6. Technicien informatique

- Collaborer avec le responsable de la sécurité de l'information et l'informer de toute situation pouvant aller à l'encontre de cette directive.

9.7. Direction des ressources humaines, communications et affaires juridiques

- Collaborer avec la direction des ressources informationnelles à l'application de cette directive.
- Suite aux analyses effectuées par le CGSI, procéder aux enquêtes appropriées.
- Proposer les mesures disciplinaires, administratives ou légales à appliquer en fonction de la gravité et des conséquences du geste posé par l'employé.
- Assurer la conservation des preuves recueillies.

9.8. Les responsables de la protection des renseignements personnels

- Collaborer avec la DRI à l'application de cette directive.
- Suite aux analyses effectuées par le CGSI, procéder aux enquêtes appropriées.
- Assurer la conservation des preuves recueillies.

9.9. Les utilisateurs

- Respecter la présente directive. En cas de doute, dans une situation donnée, la personne concernée doit consulter son supérieur sur la conduite à adopter.
- Utiliser les systèmes électroniques et le réseau Internet de manière responsable pour le travail uniquement, en respectant les règles de sécurité informationnelle.
- S'engager à n'utiliser que les équipements informatiques officiels acquis auprès des fournisseurs autorisés de biens et de services et autorisés par le service informatique.

10. Documentation connexe

- Procédure de gestion de l'utilisation d'Internet

- Formulaire d'engagement au respect de la confidentialité

Québec