Centre intégré universitaire de santé et de services sociaux de l'Estrie – Centre hospitalier universitaire de Sherbrooke
Québec

DIRECTIVE

B001–DIR-02

DIRECTIVE – UTILISATION DES SYSTÈMES ÉLECTRONIQUES

Émetteur	Présidence-direction générale adjointe
Direction responsable	Présidence-direction générale adjointe
Destinataires	L'ensemble de la communauté du CIUSSS de l'Estrie – CHUS
Entrée en vigueur	2023-06-20
Adopté par	Comité de direction **Date** 2023-06-20
Signature	Original signé par : Stéphane Tremblay Président-directeur général

Table des matières

1. Mise en contexte

Les organisations constituant le réseau de la santé et des services sociaux du Québec utilisent de plus en plus les communications électroniques. Cette utilisation doit être encadrée de façon à répondre aux besoins organisationnels et assurer la sécurité des systèmes électroniques.

Le Centre intégré universitaire de santé et de services sociaux de l'Estrie – Centre hospitalier universitaire de Sherbrooke (CIUSSS de l'Estrie – CHUS) fournit à ses employés et à ses intervenants divers outils de travail visant à les soutenir dans leurs tâches afin qu'ils puissent les accomplir plus aisément et permettre d'accroître l'efficacité de chacun.

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

La présente directive vise à informer et à sensibiliser les utilisateurs du CIUSSS de l'Estrie – CHUS à utiliser judicieusement les systèmes électroniques en définissant globalement les modalités d'une telle utilisation.

Les systèmes électroniques sont des outils de travail et ne doivent être utilisés par les employés et les intervenants qu'à cette fin, c'est-à-dire pour recevoir, transmettre ou échanger des données et des documents liés au travail, pour communiquer avec des usagers, proches d'usagers, collègues, partenaires syndicaux ou avec des fournisseurs du CIUSSS de l'Estrie – CHUS, pour effectuer des recherches sur Internet ou pour y obtenir des informations utiles pour l'organisation.

L'utilisation des systèmes électroniques comporte certains risques pour le CIUSSS de l'Estrie – CHUS par exemple, voir sa responsabilité engagée pour l'atteinte à des droits d'auteur, la diffusion de données protégées par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1), la diffusion ou la transmission de messages disgracieux, de mauvais goût, discriminatoires et/ou illégaux ou encore voir son réseau informatique compromis, piraté, ou monopolisé par une surcharge ou infecté par un virus.

Ainsi, il est primordial que l'ensemble de la communauté du CIUSSS de l'Estrie – CHUS utilise les systèmes électroniques de façon appropriée et assure la confidentialité, protège la vie privée et applique les meilleures pratiques en matière de sécurité de l'information.

2. Objectifs

En respect de la Politique de la sécurité de l'information du CIUSSS de l'Estrie – CHUS[1], les objectifs de la présente directive sont :

- de s'assurer que tous les utilisateurs du CIUSSS de l'Estrie – CHUS respectent et appliquent les règles en place afin de protéger l'information et les systèmes électroniques de manière à en assurer leur disponibilité, leur intégrité et leur confidentialité;
- d'empêcher l'utilisation inappropriée des systèmes électroniques du CIUSSS de l'Estrie – CHUS par ses utilisateurs;
- de promouvoir des habitudes et comportements judicieux et sécuritaires en matière d'utilisation des systèmes électroniques du CIUSSS de l'Estrie – CHUS, de protection des renseignements personnels et de sécurité de l'information.

[1] Intranet > Liens rapides > Bouton Sécurité de l'information.

3. Définition des termes

- **Actif informationnel** : toute information détenue ou produite, peu importe le support (électronique ou papier) notamment une banque d'information, un site Web, un système d'information, un réseau de télécommunication, un logiciel, une infrastructure, un équipement technologique ou un ensemble de ces éléments ainsi qu'une composante informatique d'un équipement médical spécialisé ou ultraspécialisé. Il est également considéré comme un actif informationnel, tout support papier contenant de l'information.
- **Confidentialité** : propriété d'une information de n'être accessible ou divulguée qu'à une personne ou à une entité désignée et autorisée. Qui se dit/se fait en confidence, qui contient des informations qui doivent demeurer secrètes. L'obligation de confidentialité est applicable à tous les utilisateurs. Cette obligation peut découler de règles éthiques, organisationnelles ou de la loi.
- **Détenteur d'actifs informationnels** : gestionnaire dont le rôle est de s'assurer de la sécurité d'actifs informationnels relevant de sa direction ou de sa responsabilité.
- **Disponibilité** : propriété d'une information d'être accessible en temps et de manière requise par une personne ou une entité désignée et autorisée.
- **Exfiltration de données** : situation dans laquelle un utilisateur autorisé extrait des données des systèmes sécurisés auxquels elles sont rattachées, et les partage avec des tiers non autorisés ou les transfère vers des systèmes non sécurisés. L'exfiltration de données peut être le fait de personnes malveillantes ou de pirates, ou elle peut être accidentelle.
- **Gestionnaire** : employé-cadre ayant des employés/salariés, contractuels ou fournisseurs sous sa responsabilité.
- **Intégrité** : propriété d'une information de ne subir aucune altération ou destruction de façon erronée ou sans autorisation.
- **Renseignement confidentiel** : une donnée ou une information dont l'utilisation et l'accès sont réservés à des personnes ou entités désignées et autorisées. Ces renseignements comprennent tout renseignement stratégique, financier, commercial ou scientifique détenu par l'établissement, ce qui inclut notamment tout renseignement dont la divulgation peut porter préjudice à un usager, à un utilisateur de l'établissement ou au CIUSSS de l'Estrie – CHUS ou à l'un de ses employés ou représentants.
- **Renseignement personnel** : les renseignements personnels sont ceux qui portent sur une personne physique et qui permettent de l'identifier.
- **Systèmes électroniques** : ordinateurs, téléphones, téléphones intelligents, tablettes numériques, boîtes vocales, télécopieurs, imprimantes multifonctions, réseaux informatiques, réseaux sans-fil, courrier électronique, outils collaboratifs, Internet ainsi que tout autre système électronique mis à la disposition des utilisateurs.
- **Télétravail** : Activité professionnelle autorisée par le gestionnaire qui s'exerce à l'extérieur des bureaux du CIUSSS de l'Estrie – CHUS, au moyen d'outils informatiques et de télécommunication.
- **Télésanté** : Ensemble des activités, services et systèmes permettant l'échange, à distance, de données liées à la santé, au moyen d'outils informatiques et de télécommunication. La télésanté est une modalité d'organisation et de dispensation de services qui crée un réseau virtuel complémentaire de services de santé et de services sociaux. Elle permet de rendre accessibles, à distance, des services cliniques communément offerts dans la programmation clinique des établissements de santé et de services sociaux pour traiter les usagers.
- **Usager** : toute personne qui a reçu, aurait dû recevoir, reçoit ou requiert des services du CIUSSS de l'Estrie – CHUS. Ce terme comprend, le cas échéant, tout représentant de l'usager au sens de l'article 12 de la *Loi sur les services de santé et les services sociaux* (RLRQ, chapitre S-4.2).
- **Utilisateur** : toute personne physique ou morale qui utilise ou qui accède à un actif informationnel du CIUSSS de l'Estrie – CHUS ou qui utilise ses systèmes électroniques. Cela comprend notamment tout employé, gestionnaire, détenteur d'actifs informationnels qui exerce sa profession au sein du CIUSSS de l'Estrie – CHUS, ainsi que tout médecin, membre du personnel de recherche, médecin résident, stagiaire

ou bénévole et toute personne qui, en vertu d'un contrat de services ou d'un mandat dispense des services pour le compte du CIUSSS de l'Estrie – CHUS, incluant les fournisseurs, partenaires, fondations, contractuels et administrateurs.

4. Champs d'application

La présente directive s'applique à tout utilisateur qui fait usage des systèmes électroniques appartenant au CIUSSS de l'Estrie – CHUS.

Elle concerne l'utilisation des systèmes électroniques mis à la disposition des utilisateurs.

5. Contenu de la directive

5.1 Propriété des systèmes électroniques

Les systèmes électroniques du CIUSSS de l'Estrie – CHUS, les droits d'utilisation des logiciels, la navigation Internet, les comptes de courrier électronique ainsi que toute information ou tout message qui est créé, envoyé, reçu, mémorisé ou téléchargé et généralement conservé par les systèmes électroniques du CIUSSS de l'Estrie – CHUS font partie intégrante des registres de l'organisation et, par le fait même, sont présumés être la propriété du CIUSSS de l'Estrie – CHUS.

5.2 Utilisation des systèmes électroniques à des fins professionnelles

Les systèmes électroniques sont mis à la disposition des utilisateurs du CIUSSS de l'Estrie – CHUS pour les fins de leur travail afin de soutenir les différentes tâches qu'ils doivent accomplir et, du même coup, accroître leur efficacité. Les systèmes électroniques du CIUSSS de l'Estrie – CHUS doivent être utilisés à des fins professionnelles seulement.

5.3 Utilisation des outils autorisés par le CIUSSS de l'Estrie – CHUS

Le CIUSSS de l'Estrie – CHUS fournit à ses utilisateurs divers outils de travail, tels que la suite collaborative Office365, visant à les soutenir dans leurs tâches. Les utilisateurs doivent faire usage des licences acquises par le CIUSSS de l'Estrie – CHUS pour s'assurer qu'ils répondent aux critères de sécurité et de confidentialité.

À titre d'exemple, l'utilisation de la licence TEAMS permet d'assurer la sécurité des échanges, ce qui n'est pas nécessairement le cas d'un autre outil de conférence Web. Aussi, l'installation d'un outil non autorisé peut contenir des codes malveillants ou virus et contaminer ensuite le réseau informatique du CIUSSS de l'Estrie – CHUS.

Dans l'éventualité qu'un système électronique a été installé sans autorisation ou aurait été compromis ou piraté, le CIUSSS de l'Estrie – CHUS se réserve le droit de désinstaller tout outil/licence sur un système électronique.

5.4 Journalisation

La journalisation permet d'assurer une traçabilité des accès et des actions posées par les utilisateurs accédant aux systèmes électroniques du CIUSSS de l'Estrie – CHUS. En outre, elle permet de détecter des incidents et des accès non autorisés ou des intrusions dans les systèmes informatiques.

Pour des fins de sécurité de l'information, ou afin de respecter des exigences légales, la plupart des actions sur les systèmes électroniques du CIUSSS de l'Estrie – CHUS sont journalisées. Ainsi, le CIUSSS de l'Estrie – CHUS se réserve le droit de faire toute vérification ou enquête sur toute irrégularité, réelle ou présumée, portée à son attention et/ou de dévoiler ces communications à toute autorité officielle ou à toute autre tierce partie, lorsque les circonstances le justifient.

5.5 Surveillance des systèmes électroniques

Toujours dans un objectif d'assurer la sécurité des systèmes électroniques, des mécanismes de surveillance sont mis en place dans le but d'assurer la protection de ceux-ci. Conséquemment, le CIUSSS de l'Estrie – CHUS pourrait, lorsque les circonstances le justifient, surveiller, accéder, récupérer, lire les communications des utilisateurs qui ont été créées, envoyées, reçues ou mémorisées par les systèmes électroniques du CIUSSS de l'Estrie – CHUS, et ce, sans avis préalable aux expéditeurs ou aux destinataires de telles communications.

En outre, le CIUSSS de l'Estrie – CHUS se réserve le droit de faire toute vérification ou enquête sur toute irrégularité, réelle ou présumée, portée à son attention et/ou de dévoiler ces communications à toute autorité officielle ou à toute autre tierce partie, lorsque les circonstances le justifient.

Les principes et conditions guidant le CIUSSS de l'Estrie – CHUS dans sa décision de procéder à la surveillance des systèmes électroniques sont notamment les suivants :

- La surveillance doit poursuivre un objectif important et sérieux, soit d'assurer la sécurité et l'utilisation judicieuse des systèmes électroniques du CIUSSS de l'Estrie – CHUS;
- La surveillance doit être fondée sur des motifs raisonnables;
- Elle doit respecter le critère de proportionnalité, c'est-à-dire qu'elle doit qu'elle doit être effectuée à l'aide de moyens raisonnables et proportionnés à la nature et à la complexité de la situation afin de rencontrer son objectif.

5.6 Responsabilités des utilisateurs

- Protection des informations confidentielles

  L'utilisateur doit en tout temps assurer la confidentialité des informations, qu'elles soient de nature administrative ou clinique, échangées au moyen des systèmes électroniques. Ainsi, il est de sa responsabilité d'utiliser les moyens mis à sa disposition pour communiquer, échanger ou recevoir des informations confidentielles. À titre d'exemple, sans chiffrement[2], la confidentialité d'un message envoyé par courrier électronique ainsi que celle de ses pièces jointes ne peuvent pas, par défaut, être assurée.

  De même, l'utilisateur doit respecter la confidentialité des informations auxquelles il a accès dans l'exercice de ses fonctions. Il est notamment interdit de consulter, de divulguer ou d'imprimer des informations, que ce soit pour lui-même, l'un de ses proches ou toute autre personne, si l'activité n'est pas nécessaire à l'exercice de ses fonctions professionnelles.

  L'utilisateur doit faire usage de ses codes d'utilisateur et mots de passe pour lesquels il a obtenu une autorisation. Les mots de passe doivent être conservés de façon sécuritaire. À moins de circonstances exceptionnelles hors de son contrôle, celui-ci est entièrement responsable des activités résultant de leur usage et doit prendre les mesures appropriées pour les protéger.

  Les tâches effectuées avec un code d'utilisateur sont réputées avoir été faites par le détenteur officiel de ce code et c'est la responsabilité du détenteur de ne pas le divulguer à autrui.

- Vigilance en tout temps

  Les cybercriminels intensifient l'utilisation de l'ingénierie sociale pour exploiter le « facteur humain », c'est-à-dire la curiosité et la confiance naturelle qui poussent des utilisateurs bien intentionnés à cliquer, télécharger, installer des fichiers malveillants ou encore divulguer des informations stratégiques ou confidentielles. En effet, qu'elles visent une base très large ou hautement ciblée, qu'elles soient véhiculées par l'Internet, la messagerie électronique, les médias sociaux, l'infonuagique ou d'autres vecteurs de propagation motivés par l'appât du gain ou par d'autres intérêts, les tactiques d'ingénierie sociale exploitées dans le cadre d'attaques sont de plus en plus présentes et dangereuses.

[2] Pour connaitre la façon d'utiliser le chiffrement : Intranet > Liens rapides > Bouton Sécurité de l'information.

Ainsi, compte tenu de ces menaces informatiques, les utilisateurs doivent continuellement être vigilants, notamment lorsqu'ils reçoivent des courriels non sollicités ou qu'ils naviguent sur Internet.

Les utilisateurs doivent signaler les incidents liés à la sécurité de l'information dans les meilleurs délais au Centre de services de la DRIT selon la procédure en vigueur[3].

- **Respect du droit à l'image**

  En vertu du cadre juridique applicable, le fait de photographier ou filmer un individu ou un usager sans son consentement explicite peut constituer une violation du droit à la vie privée.

  Si, dans l'exercice de leur fonction, les utilisateurs doivent filmer ou photographier un usager, cela doit se faire dans le cadre d'un protocole clair établi avec son gestionnaire à cet effet, avec les systèmes électroniques autorisés par le CIUSSS de l'Estrie – CHUS et en ayant obtenu, au préalable, le consentement écrit de l'usager.

- **Utilisation des médias sociaux et diffusion d'information sur Internet**

  Une utilisation judicieuse des réseaux sociaux s'impose puisque cet espace public peut donner lieu, notamment, à des dérapages et à des bris de confidentialité. À cet effet, il est interdit de diffuser auprès des médias et dans les réseaux sociaux (Facebook, Twitter, Instagram, Snapchat, etc.) tous renseignements confidentiels et sensibles du CIUSSS de l'Estrie – CHUS, tous renseignements concernant des usagers ou des employés du CIUSSS de l'Estrie – CHUS ou des informations permettant de les identifier directement ou indirectement par quelque moyen que ce soit : vidéos, images, noms ou autres, ainsi que tout renseignement qui va à l'encontre des intérêts du CIUSSS de l'Estrie – CHUS.

  Au besoin, l'utilisateur doit se référer au Règlement interne sur l'utilisation des médias sociaux[4].

  De même, les utilisateurs ne peuvent diffuser ou publier, sur Internet ou sur tout autre environnement public, de l'information concernant le CIUSSS de l'Estrie – CHUS, sauf s'ils y sont spécifiquement autorisés. À titre indicatif, certaines personnes désignées sont autorisées à des fins professionnelles et pour les besoins d'affaires du CIUSSS de l'Estrie – CHUS, notamment les édimestres du CIUSSS de l'Estrie – CHUS qui mettent en ligne du contenu et effectuent une veille stratégique.

- **Télétravail**

  Sur le plan de la sécurité de l'information, lorsqu'un utilisateur est en télétravail, il est nécessaire qu'il adopte un comportement sécuritaire et similaire à celui qu'il adopterait s'il était physiquement présent au bureau. Par exemple, les utilisateurs doivent prendre les mesures appropriées afin d'éviter toute utilisation non autorisée de son équipement ou le vol de ce dernier, ce qui inclut le fait ne pas laisser son appareil sans surveillance ou non verrouillé lors d'absence.

  D'autre part, si un jeton de téléacccès a été octroyé, le numéro d'identification personnel (NIP) de celui-ci ne doit être en aucun cas partagé ou affiché et le jeton ne doit être utilisé qu'avec un équipement fourni par le CIUSSS de l'Estrie – CHUS.

  Au besoin, l'utilisateur doit se référer à la *Politique sur le télétravail*[5].

- **Télésanté**

  Le CIUSSS de l'Estrie – CHUS s'inscrit dans une démarche de modernisation afin de pérenniser la télésanté et de l'intégrer dans les services cliniques offerts aux usagers et à leurs proches. La pratique de la télésanté doit cependant être encadrée au sein du CIUSSS de l'Estrie – CHUS en définissant des orientations et responsabilités claires pour les parties prenantes.

[3] Intranet > Liens rapides > Bouton Centre de services DRIT.

[4] Intranet > CIUSSS de l'Estrie - CHUS > Règlements, politiques, directives et procédures > Règlement interne sur l'utilisation des médias sociaux.

[5] Intranet > CIUSSS de l'Estrie - CHUS > Règlements, politiques, directives et procédures > Politique sur le télétravail.

Les parties prenantes doivent appliquer les bonnes pratiques de télésanté et au besoin elles doivent se référer à la *Politique de télésanté*[6].

En outre, le professionnel clinique et médical doit s'assurer d'acquérir et de maintenir les compétences requises pour offrir les soins et services par le biais de la modalité de télésanté, et ce, afin d'offrir une prestation de travail équivalente à celle qu'il livre à partir d'une modalité traditionnelle (en présentiel ou par téléphone).

- **Utilisation de réseaux sans-fil (Wi-Fi)**

  Les réseaux sans-fil publics font souvent l'objet de piratage. Les utilisateurs doivent faire usage des réseaux sans-fil sécuritaires, notamment les réseaux domestiques ou organisationnels comme ceux d'autres organisations gouvernementales. De plus, si le réseau domestique Wi-Fi est utilisé pour faire du télétravail, celui-ci doit être protégé notamment avec un mot de passe robuste associé à un mécanisme de chiffrement fort (protocole WPA3/WPA2 et chiffrement AES).

  Un ordinateur utilisé en télétravail qui accède à Internet avec un câble réseau (et non par Wi-Fi) doit être relié à un routeur et non branché directement dans le modem du fournisseur Internet.

- **Enregistrement des fichiers**

  L'enregistrement des fichiers (ex. : Word, Excel) doit être effectué afin que ceux-ci soient pris en sauvegarde pouvant ainsi être restaurés advenant un incident de sécurité. Par exemple, l'enregistrement sur les serveurs de fichiers du CIUSSS de l'Estrie – CHUS (ex. : lecteur B) est recommandé contrairement à un enregistrement sur le disque dur local de l'ordinateur.

  Dans l'éventualité d'un incident de sécurité (ex. : introduction de virus informatique), les fichiers sauvegardés dans le disque dur local de l'ordinateur (ex. : fichiers de téléchargements, Bureau) ne seront pas récupérés.

  D'autre part, en cas de vol de l'ordinateur, les informations enregistrées localement se retrouvent entre les mains du malfaiteur, pouvant ainsi mener à des conséquences graves, notamment à un vol d'identité, à l'atteinte de la vie privée et des bris de confidentialité.

5.7 Activités proscrites

- **Droits de propriété intellectuelle**

  Les utilisateurs ne doivent pas télécharger, utiliser ou transmettre du matériel breveté ou protégé par les droits d'auteur ou les marques de commerce sans que les droits aient été acquis légalement. Il revient à l'utilisateur de s'assurer de vérifier qu'il puisse utiliser ce matériel légalement.

- **Partage de code d'utilisateur et de mot de passe**

  L'utilisation de codes d'utilisateur et mots de passe sont des outils privilégiés permettant d'atteindre plusieurs objectifs visés par la présente directive dont le contrôle de l'accès à certaines ressources, de même que la confidentialité des fichiers emmagasinés sur le réseau du CIUSSS de l'Estrie – CHUS. Conséquemment, l'utilisateur, à moins de circonstances exceptionnelles, ne doit jamais utiliser le code d'utilisateur ou le mot de passe d'une autre personne. L'utilisation du code d'utilisateur et du mot de passe d'un tiers est interdite et pourrait même être considérée comme de l'usurpation d'identité selon le cas.

- **Utilisation des systèmes électroniques par un tiers**

  Les utilisateurs ne peuvent pas permettre directement ou indirectement à une tierce personne, sans autorisation expresse, d'accéder ou d'utiliser les systèmes électroniques du CIUSSS de l'Estrie – CHUS.

[6] Intranet > CIUSSS de l'Estrie - CHUS > Règlements, politiques, directives et procédures > Politique de télésanté.

- **Virus et activités illicites**

  Les utilisateurs ne doivent pas utiliser les systèmes électroniques du CIUSSS de l'Estrie – CHUS pour télécharger en amont ou en aval ou par d'autres façons, transmettre des informations ou des contenus illégaux.

  Il est interdit de naviguer sur des sites malveillants ou réputés malveillants (ex. : DarkWeb).

  Il est strictement interdit d'introduire intentionnellement, de propager ou de développer des virus dans ou avec les systèmes électroniques du CIUSSS de l'Estrie – CHUS ou de procéder à des altérations illicites des systèmes électroniques.

  De même, il est interdit de posséder, utiliser ou diffuser un mécanisme logiciel ou matériel sous forme d'outil (logiciel espion ou piratage informatique) ou utiliser une stratégie ou un système quelconque (ex. : VPN) qui permet de désactiver, détruire ou de contourner quelque mesure de sécurité que ce soit mise en place pour protéger la confidentialité ou la sécurité des systèmes électroniques.

  Les utilisateurs ne doivent pas pirater ou commettre une action frauduleuse aux programmes, aux logiciels ou aux données du CIUSSS de l'Estrie – CHUS. De même, aucun utilisateur ne peut prêter son concours à une telle activité. Lorsqu'un utilisateur est témoin ou soupçonne une telle situation, il doit la signaler au Centre de services de la DRIT selon la procédure en vigueur[7].

- **Téléchargement de programme**

  Les utilisateurs ne doivent pas télécharger, d'Internet ou de toute autre source externe, tout type de programme, logiciel, utilitaire ou extension de navigateur dont l'usage qui ne soit pas expressément autorisé par le CIUSSS de l'Estrie – CHUS. Il revient à l'utilisateur de s'assurer que le produit soit autorisé par le CIUSSS de l'Estrie – CHUS. À ce titre, il peut communiquer auprès du Centre de services de la DRIT selon la procédure en vigueur[8].

  Aucun utilisateur ne doit, en utilisant les systèmes électroniques mis à sa disposition par le CIUSSS de l'Estrie – CHUS, télécharger, distribuer ou copier des logiciels ou des données qu'il sait, soupçonne ou devrait raisonnablement soupçonner être piratés, malveillants ou non sécuritaires pour les systèmes électroniques. Dans le doute, l'utilisateur est invité à s'adresser au Centre de services de la DRIT selon la procédure en vigueur[9].

- **Fichiers personnels**

  L'enregistrement de documents personnels crée une surcharge qui ralentit considérablement les systèmes électroniques, particulièrement lorsqu'il s'agit de musique, de vidéos, ou de photos. Ceci affecte le bon déroulement des activités du CIUSSS de l'Estrie – CHUS et engendre des coûts importants (par exemple, pour l'achat de serveurs de fichiers supplémentaires pour pallier un manque d'espace disque).

  De plus, le CIUSSS de l'Estrie – CHUS n'est pas responsable de la sauvegarde ni de la récupération des fichiers personnels, et ce, peu importe la plateforme d'enregistrement (ex. : la reconfiguration d'un ordinateur suite à une infection par un virus informatique).

  Toutes les plateformes de sauvegarde sont réservées uniquement pour la conservation de documents requis dans le cadre de l'exercice des fonctions professionnelles de l'utilisateur. Le CIUSSS de l'Estrie – CHUS pourrait, sans préavis, supprimer tout document personnel conservé sur un système électronique de celui-ci lorsque les circonstances le justifient.

- **Surcharge du réseau**

  Les utilisateurs ne doivent pas faire usage des systèmes électroniques du CIUSSS de l'Estrie – CHUS d'une manière susceptible de désactiver ou de surcharger n'importe quel système ou réseau informatique. Il est interdit d'utiliser du contenu multimédia en continu (ex. : musique en ligne) ou de télécharger ce même

[7] Intranet > Liens rapides > Bouton Centre de services DRIT.

[8] Intranet > Liens rapides > Bouton Centre de services DRIT.

[9] Intranet > Liens rapides > Bouton Centre de services DRIT.

type de contenu par le réseau Internet si ce contenu n'est pas requis à des fins professionnelles et/ou qu'il n'est pas autorisé par le CIUSSS de l'Estrie – CHUS.

- **Utilisation éthique des technologies de l'information**

  Il est interdit d'afficher ou de télécharger des données de sites Internet aux contenus sexuellement explicites ou autrement intimidants, hostiles, offensants, discriminatoires ou diffamatoires.

  Aucun utilisateur ne doit télécharger, enregistrer, archiver, afficher, posséder, transmettre ou distribuer toute image, tout écrit ou message sonore à connotation sexuelle ou de nature disgracieuse, offensante ou discriminatoire fondé sur la race, la couleur, le sexe, la grossesse, l'orientation sexuelle ou de genre, l'état civil, l'âge, la religion, les convictions politiques, la langue, l'origine ethnique ou nationale, les conditions sociales ou le handicap, par le biais des systèmes électroniques du CIUSSS de l'Estrie – CHUS.

  Sans restreindre la généralité de ce qui précède, les systèmes électroniques du CIUSSS de l'Estrie – CHUS ne doivent pas être utilisés à des fins politiques, pour participer à des jeux de hasard ou de paris, pour créer ou distribuer des chaînes de lettres, pour s'abonner à des listes d'envoi non reliées aux activités du CIUSSS de l'Estrie – CHUS ou, pour toute autre pratique non conforme aux politiques et directives de celui-ci.

- **Sites Web et courriels douteux**

  Les utilisateurs ne doivent pas tenter d'accéder à un site Web au moyen de liens Internet dont l'usage est inconnu ou cliquer des liens ou ouvrir des documents attachés par courrier électronique dont la provenance est inconnue ou douteuse. En cas de doute, les utilisateurs doivent contacter le Centre de services de la DRIT selon la procédure en vigueur[10].

- **Envoi massif de messages**

  Les utilisateurs ne peuvent pas faire usage des systèmes électroniques du CIUSSS de l'Estrie – CHUS, notamment le courrier électronique, pour des envois massifs de messages pour des fins de sondage, de publicité ou d'événement sans relation avec les activités de l'organisation.

- **Utilisation de la fonction photo des téléphones intelligents**

  Les utilisateurs ne doivent pas utiliser la fonction photo des téléphones intelligents pour conserver, échanger ou acheminer des données cliniques ou confidentielles. Sans chiffrement, les informations ainsi collectées ou échangées ne bénéficient d'aucune protection et peuvent être interceptées ou utilisées à d'autres fins. En cas de doute, l'utilisateur peut communiquer auprès du Centre de services de la DRIT selon la procédure en vigueur[11].

- **Utilisation d'un ordinateur personnel sur le réseau du CIUSSS de l'Estrie – CHUS**

  Les utilisateurs ne doivent pas faire usage de leur ordinateur personnel sur le réseau filaire du CIUSSS de l'Estrie – CHUS.

- **Médias amovibles (périphériques externes)**

  Les médias amovibles, tels que les clés USB ou disques durs externes, sont des sources importantes de fuites d'information. Les utilisateurs ne doivent pas faire usage d'un média amovible sans chiffrement[12] s'il contient des renseignements confidentiels.

  Par ailleurs, les médias amovibles représentent des vecteurs importants d'attaques et de propagation de virus informatiques. Conséquemment, les utilisateurs ne doivent pas utiliser ces médias qu'à des fins professionnelles et avec les équipements du CIUSSS de l'Estrie – CHUS. L'utilisation de médias amovibles personnels est non recommandée.

[10] Intranet > Liens rapides > Bouton Centre de services DRIT.

[11] Intranet > Liens rapides > Bouton Centre de services DRIT.

[12] Pour connaitre la façon d'utiliser un média amovible avec chiffrement : Intranet > Liens rapides > Bouton Sécurité de l'information.

- **Exfiltration de données hors des systèmes informatiques du CIUSSS de l'Estrie – CHUS**

  Les utilisateurs ne doivent pas exfiltrer les données du CIUSSS de l'Estrie – CHUS de façon non autorisée, notamment par le biais de comptes de messagerie personnels, de stockage dans l'infonuagique (ex. : Dropbox), d'imprimantes, de sites de partage de fichiers (ex. : WeTransfer) ou de médias amovibles (ex. : clé USB).

  Les données n'ont alors aucune protection, sinon minime, comme celle offerte sur les systèmes informatiques du CIUSSS de l'Estrie – CHUS.

6. Rôles et responsabilités

- Tout utilisateur autorisé à avoir accès aux actifs informationnels du CIUSSS de l'Estrie – CHUS assume des responsabilités particulières en matière de sécurité de l'information, notamment quant à la protection de l'information et des systèmes électroniques.
- La sécurité de l'information est une responsabilité partagée par tous les utilisateurs et chaque utilisateur est personnellement responsable des actes qu'il pose.
- L'utilisateur a l'obligation de protéger les actifs informationnels mis à sa disposition par le CIUSSS de l'Estrie – CHUS. À cette fin, il doit prendre connaissance de la présente directive, des procédures et autres lignes de conduite en découlant, y adhérer et prendre l'engagement de s'y conformer.
- Un utilisateur qui constate ou soupçonne une situation qui contrevient à la présente directive ou une infraction pouvant compromettre la sécurité des actifs informationnels doit la signaler promptement auprès de son supérieur immédiat ou au chef de la sécurité de l'information organisationnelle du CIUSSS de l'Estrie – CHUS, le cas échéant, ou par le biais du formulaire de signalement concernant la sécurité de l'information[13].

7. Dispositions finales

7.1 Sanctions

Toute personne, physique ou morale, assujettie à la présente directive qui y contrevient ou déroge aux procédures et autres lignes de conduite qu'elle contient, s'expose, selon le cas, à des mesures disciplinaires, administratives ou contractuelles en fonction de la gravité de son geste.

7.2 Version antérieure

La présente mise à jour remplace la version adoptée en juin 2016 par le Comité de sécurité de l'information.

7.3 Prochaine révision

La présente directive doit faire l'objet d'une révision au plus tard dans les quatre (4) années suivant son entrée en vigueur.

[13] Intranet > Liens rapides > Bouton Sécurité de l'information.

Annexe A - Historique des versions

Description	Auteur/Responsable	Date / Période
Mise à jour de la directive	Julie Nadeau, conseillère en gouvernance de la sécurité de l'information (PDGA)	06-06-2022
Révision avec modification	Myriam Bourque, responsable de la sécurité de l'information (PDGA)	14-06-2022
Révision avec modification	Membres du comité de la sécurité de l'information, gestion des accès et protection des renseignements personnels	09-11-2022
Révision avec modification	Marianne Bellefleur, avocate (DRHCAJ)	23-05-2023
Révision avec modification	Samuel Proulx, avocat (DRHCAJ)	29-05-2023
Révision avec modification	Équipe du service de la Sécurité de l'information	07-06-2023
Adoption	Comité de direction du CIUSSS de l'Estrie - CHUS	20-06-2023