Centre intégré de santé et de services sociaux de la Gaspésie Québec	**DIRECTIVE**
TITRE :	Sécurité de l'information
NUMÉRO :	CGA-2018-111
REMPLACE DOCUMENT(S) SUIVANT(S), S'IL Y A LIEU :	

PERSONNEL VISÉ :	☒ gestionnaires ☒ personnel de soutien ☒ soins/services aux patients/clients Précisez, s'il y a lieu :
PERSONNE RESPONSABLE :	Alain Vézina
DIRECTION RESPONSABLE :	Direction des ressources informationnelles

HISTORIQUE DES VERSIONS					
Version :	Préparée par :	**Vérifiée par :**	**Approuvée par :**	**Entrée en vigueur :**	**Archivée :**
1RE	ALAIN VEZINA	**ALAIN VEZINA**	**CONSEIL D'ADMINISTRATION**	**13 JUIN 2018**	
2E					

RÉVISION ANNUELLE **Prochaine révision prévue le : 13 juin 2021**	
Date de réalisation de la révision	

N. B. : *Dans ce texte, le masculin englobe les deux genres et est utilisé pour alléger le texte.*

CONTEXTE

La présente directive sur la sécurité de l'information regroupe les principales normes et règles qui doivent être observées par tous les utilisateurs des actifs informationnels ou de télécommunication du CISSS de la Gaspésie, tout particulièrement ceux qui ont accès à des renseignements nominatifs ou à caractère confidentiel.

Ce sommaire se veut un aide-mémoire afin que tous les utilisateurs soient en mesure d'intégrer ces normes et règles dans l'exercice de leurs fonctions.

RESPONSABILITÉS DES UTILISATEURS

Les utilisateurs:

- Doivent prendre connaissance de la politique et de la directive sur la sécurité de l'information et les respecter;
- Doivent aviser leur supérieur immédiat ou le responsable de la sécurité des actifs informationnels dès qu'ils constatent un défaut de respecter les normes prévues à la politique;
- Sont responsables de leurs manquements.

De façon plus précise et explicite concernant le réseau informatique, les utilisateurs :

- Ne peuvent qu'utiliser l'identifiant, les codes d'accès et/ou les mots de passe pour lesquels ils ont obtenu une autorisation d'usage. Tous ces droits sont strictement confidentiels;
- Doivent utiliser le réseau informatique de manière efficace et pour des tâches reliées à l'exercice de leurs fonctions;
- Doivent respecter le caractère nominatif et confidentiel des données auxquelles ils ont accès;
- Ne peuvent procéder à l'enregistrement de données nominatives ou confidentielles sur un support externe sans que ceux-ci soient protégés par un mot de passe;
- Ne peuvent procéder à l'installation de logiciels ou de périphériques sur les postes du réseau;
- Ne peuvent procéder au raccordement d'équipements personnels (ordinateurs, clé USB, etc.) au réseau de l'établissement.

De façon plus précise et explicite concernant Internet, les utilisateurs :

- Doivent utiliser Internet afin d'obtenir des informations utiles et requises dans le cadre de leurs fonctions;
- Ne peuvent se servir des facilités d'accès à Internet pour:
  - télécharger des logiciels;
  - participer à des concours ou à des sondages qui ne sont pas dans le cadre de leurs fonctions;
  - écouter de la musique;
  - accéder à tout site à caractère sexuel, haineux, raciste ou socialement inacceptable, etc.
- Doivent utiliser le réseau de l'établissement en conformité avec la politique sur les médias sociaux.

De façon plus précise et explicite concernant l'utilisation du courrier électronique, les utilisateurs :

- Doivent limiter l'utilisation de courrier électronique aux messages et aux fichiers attachés qui sont en lien avec les fonctions occupées au sein de l'établissement;
- Doivent informer rapidement le service informatique de tout courriel alertant de la présence possible d'un virus informatique;
- Ne peuvent se servir du courrier électronique pour:
  - transmettre un courriel alertant la présence possible d'un virus informatique;
  - participer à une chaîne de lettres pour effectuer de la publicité ou de la vente pyramidale ou pour faire des envois massifs de messages sans autorisation.

De façon plus précise et explicite concernant les télécopieurs, les utilisateurs :

- Doivent utiliser les télécopieurs afin de transmettre des informations utiles ou requises dans le cadre de leurs fonctions;
- Doivent assurer la confidentialité de toute transmission d'information nominative ou à caractère confidentiel.

CONCLUSION

En conclusion, et ce, en conformité avec le « *Cadre global de gestion des actifs informationnels appartenant aux organismes du réseau de la santé et des services sociaux* », volet sur la sécurité, le CISSS de la Gaspésie :

- Utilise des logiciels pouvant permettre de contrôler et d'enregistrer toute utilisation d'Internet faite à partir de son réseau informatique;
- Analyse, évalue, selon les besoins, l'usage du réseau informatique et du courrier électronique.

Tout membre du personnel qui contrevient à la politique est passible, en plus des pénalités prévues aux différentes législations, de :

- Mesures disciplinaires ou administratives;
- Annulation sans avis de certains droits d'accès aux équipements et services visés par la présente politique;
- Remboursement au CISSS de la Gaspésie de toute somme que ce dernier serait dans l'obligation de défrayer à la suite d'une utilisation non autorisée, frauduleuse ou illicite de ses services ou de ses actifs informationnels et de télécommunication.

PROCESSUS DE CONSULTATION INSTITUTIONNELLE ET PROFESSIONNELLE
SELON LA PERTINENCE

Comités	**Date**
☐ Comité exécutif du conseil des infirmières et infirmiers (CECII)	N/A
☐ Comité exécutif du conseil multidisciplinaire (CECM)	N/A
☐ Comité exécutif du conseil des médecins, dentistes et pharmaciens (CECMDP)	N/A
☒ Comité de direction	2018-05-19
☒ Conseil d'administration	2018-06-13
☐ Autre(s), précisez	N/A