Centre intégré de santé et de services sociaux de la Montérégie-Centre
Québec

NUMÉRO : DRIM-101

TITRE : Politique de sécurité des ressources informationnelles	
RESPONSABLE : Direction des ressources informationnelles de la Montérégie (DRIM)	**ÉMISE LE : 2022-09-22**
ADOPTÉE PAR : Conseil d'administration	**DERNIÈRE RÉVISION :** -
POLITIQUE [X] **PROCÉDURE** [ ]	

1 PRÉAMBULE

La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* oblige les organismes du réseau de la santé et des services sociaux à mettre en œuvre les activités nécessaires, afin de répondre au cadre normatif du RSSS en sécurité de l'information.

En 2015, le ministère de la Santé et des Services sociaux a ratifié une nouvelle politique provinciale et un cadre de gestion sur la sécurité de l'information. La Loi sur la santé et les services sociaux, qui détermine le rôle d'un organisme de santé, traite également de la sécurité des ressources informationnelles (RI) puisque l'utilisation des technologies de l'information par les organismes de santé et des services sociaux est essentielle à la réalisation de leurs missions. Par conséquent, l'utilisation de cette information doit être adéquate et faire l'objet d'une protection en lien avec sa valeur.

L'organisme détient sous sa responsabilité des renseignements personnels et confidentiels ; ce qui exige une vigie rigoureuse puisque nous devons respecter plusieurs lois et règles particulières émises régulièrement.

La présente politique oriente l'organisme en matière de sécurité. Elle détermine pour l'ensemble des utilisateurs, les comportements à adopter afin de s'assurer de l'utilisation appropriée des ressources informationnelles (RI) et des informations.

La protection des ressources informationnelles s'articule autour de quatre grands axes, à savoir : Disponibilité, intégrité, confidentialité et authentification (DIC-A).

2 CHAMPS D'APPLICATION

2.1 PERSONNES VISÉES

La présente politique vise :

- Toute personne qui exerce des fonctions ou sa profession au sein de l'organisation à titre d'employé syndiqué ou non syndiqué incluant entre autres : les membres de la haute direction, les gestionnaires, les membres du CMDP (Conseil des médecins, dentistes et pharmaciens), les professionnels, les employés, les étudiants, les résidents, les membres du Conseil d'administration (CA) ;
- Toute personne qui agit à titre de bénévole, stagiaire rémunéré ou non, et contractuel ;
- Toute personne physique ou morale dûment autorisée à interagir avec les ressources informationnelles détenues par l'organisation (héberger, supporter, développer, intégrer, gérer, sécuriser ou exploiter).

2.2 RESSOURCES INFORMATIONNELLES VISÉES

Toutes les ressources informationnelles sous la responsabilité de la DRIM sont visées par la présente politique. Qu'il s'agisse de supports numériques, de bases de données, d'équipements informatiques, de réseaux informatiques ou de télécommunication ou des autres technologies de l'information d'un des CISSS de la Montérégie (Est, Centre et Ouest).

Cette section présente une liste, non exhaustive, des types de ressources informationnelles sous la responsabilité de la Direction des ressources informationnelles de la Montérégie (DRIM), notamment :

Ressources matérielles :

- Équipements des infrastructures informatiques (serveurs, commutateurs, etc.) ;
- Postes de travail et périphériques (ordinateurs, portables, etc.) ;
- Réseau informatique (filaire et sans fil « Wi-Fi ») ;
- Appareils de téléphonie mobile ;
- Appareils de téléphonie de bureau.
- Appareils d'impression et de numérisation ;

Ressources logicielles :

- Systèmes d'exploitation ;
- Logiciels de productivité et de bureautique ;
- Systèmes d'information administratifs, clinico-administratifs et cliniques ;
- Systèmes d'information hébergés en « infonuagique » sur l'Internet ;
- Système de messagerie provincial (Outlook) ;
- Autres outils collaboratifs mis à la disposition des utilisateurs (ex. : suite Office 365).

Dans le cas où les ressources/équipements ne sont pas sous la responsabilité de la DRIM, mais sont connectées/reliées au réseau informatique, leur détenteur (propriétaire) doit s'assurer qu'elles sont conformes aux exigences de sécurité en vigueur. La DRIM se réserve le droit de demander un audit sur ces ressources, notamment :

- Certains appareils biomédicaux ;
- Certaines solutions en infonuagique utilisées par des secteurs sans validation préalable de l'équipe sécurité de la DRIM ;
- Certains appareils des services techniques :
  - sécurité

- stationnement
- climatisation et chauffage
- etc.

2.3 ACTIVITÉS VISÉES

Toutes les activités impliquant la manipulation ou l'utilisation sous toutes formes des ressources informationnelles sous la responsabilité de la DRIM sont visées par la présente politique, que les activités soient conduites dans les locaux de l'organisation ou dans un autre endroit (à distance).

3 CADRE JURIDIQUE ET ADMINISTRATIF

La Politique de sécurité des ressources informationnelles s'inscrit dans un contexte régi notamment par :

- *Loi modifiant l'organisation et la gouvernance du réseau de la santé et des services sociaux* notamment par l'abolition des agences régionales (chapitre O-7.2) ;
- *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, chapitre G-1.03, a. 10 et 12) ;
- *Loi sur le ministère de la Santé et des Services sociaux* (RLRQ, chapitre M-19.2, a. 5,2 et 5,4) ;
- *Directive sur la sécurité de l'information gouvernementale* (Décret 7-2014 du 15 janvier 2014) ;
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A -21,1 2018) ;
- *Loi sur la protection des renseignements personnels et les documents électroniques* ;
- *Loi concernant le partage de certains renseignements de santé, qui encadre particulièrement l'utilisation du Dossier Santé Québec* ;
- *Règle particulière sur la sécurité organisationnelle* - MSSS 2017-06-27 ;
- *Règle particulière sur les domaines de confiance et leurs interconnexions* - MSSS 2017-06-27 ;
- *Règle particulière sur les niveaux de confiance de l'authentification* - MSSS 2013-06-20.

Documents d'encadrement connexes :

Ce document précise les principales exigences en sécurité des ressources informationnelles et s'inscrit dans une perspective holistique de sécurité de l'information, incluant notamment :

- MSSS-POL01 *Politique provinciale de la sécurité de l'information* — 2015-08-17 ;
- MSSS-DIR01 *Directive de déclaration des incidents de sécurité* — 2015-08-17 ;
- MSSS-DIR03 *Directive sur la cybersécurité* — 2022-03 ;
- MSSS05-005 *Utilisation éthique des TI* — 2008-01-08 ;
- *Termes et conditions d'utilisation des outils de collaboration* V0.9 — MSSS 2020-04-20.

4 DÉFINITIONS

Actif informationnel :	Une banque d'informations, un système d'information, un réseau de télécommunication, une infrastructure technologique ou un ensemble de ces éléments.

Ressource informationnelle :	Une ressource utilisée par une entreprise ou une organisation, dans le cadre de ses activités de traitement de l'information, pour mener à bien sa mission, pour la prise de décision, ou encore pour la résolution de problèmes. **Note** : Une ressource informationnelle peut être une ressource humaine, matérielle ou financière directement affectée à la gestion, à l'acquisition, au développement, à l'entretien, à l'exploitation, à l'accès, à l'utilisation, à la protection, à la conservation et à la destruction des éléments d'information. Une ressource peut donc être une personne, un fichier ou le système informatique lui-même. La plupart du temps, ces termes sont utilisés au pluriel. Ils désignent alors un ensemble de ressources qui peuvent être répertoriées dans l'actif informationnel de l'organisation. *(Référence : Thésaurus du Gouvernement du Québec.)*
Code malicieux	Les codes malicieux ou logiciels malveillants sont des logiciels qui infectent un système informatique à l'insu de son utilisateur en exploitant des vulnérabilités humaines ou techniques.
Cyberattaque	Incident caractérisé par un accès non autorisé et mal intentionné visant principalement à compromettre la confidentialité, l'intégrité ou la disponibilité de l'information ou des infrastructures technologiques.
Incident	Tout événement qui ne fait pas partie du fonctionnement standard d'un service et qui cause, ou peut causer, une interruption ou une diminution de la qualité de service.
Incident de sécurité	Un ou plusieurs événements liés à la sécurité de l'information, indésirable(s) ou inattendu(s), présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la sécurité de l'information (disponibilité, intégrité ou confidentialité). Un incident de sécurité de type « Comportement inapproprié » est un incident caractérisé par une négligence, une erreur, une omission ou le non-respect des règles de sécurité (Référence : MSSS-DIR01 Déclaration des incidents de sécurité — 2015-08-17).
Utilisateur	Toute personne qui exerce des fonctions ou sa profession au sein de l'organisation à titre d'employé syndiqué ou non syndiqué incluant entre autres : les membres de la haute direction, les gestionnaires, les membres du CMDP (Conseil des médecins, dentistes et pharmaciens), les professionnels, les employés, les étudiants, les résidents, les membres du Conseil d'administration (CA). Toute personne

qui agit à titre de bénévole, stagiaire rémunéré ou non, et contractuel. Toute personne physique ou morale dûment autorisée à interagir avec les ressources informationnelles détenues par l'organisation (héberger, supporter, développer, intégrer, gérer, sécuriser ou exploiter).

5 OBJECTIFS

Les informations contenues dans la présente politique contribueront notamment à l'atteinte des objectifs suivants :

- assurer le respect des obligations impactant la dimension technologique de la sécurité de l'information stipulée dans le cadre normatif du RSSS ;
- prévenir l'utilisation inappropriée des technologies des ressources informationnelles visées par la politique ;
- aviser les utilisateurs de l'existence de certaines mesures de contrôle.

6 RÔLES ET RESPONSABILITÉS

6.1 CONSEIL D'ADMINISTRATION

- Adopte la présente politique.

6.2 COMITÉ DE DIRECTION

- Recommande l'adoption de la présente politique.
- Veille à ce que soient déployés les moyens nécessaires afin de s'assurer du respect et de l'application de la présente politique par l'ensemble des directions.

6.3 DIRECTEURS ET GESTIONNAIRES

- Sensibilisent les membres de leur équipe à la présente politique ;
- Responsables de l'application de la présente politique dans leur équipe ;
- Appliquent les mesures administratives ou disciplinaires, au besoin ;
- Avisent le responsable de la sécurité des ressources informationnelles de la DRIM de toute situation jugée à risque ou contrevenant à la présente politique ;

6.4 DIRECTION DES RESSOURCES INFORMATIONNELLES DE LA MONTÉRÉGIE (DRIM)

- Assure le suivi et la mise à jour de la présente politique ;
- Assure le suivi concernant toute situation portée à sa connaissance qui est susceptible de contrevenir à la présente politique ;

6.5 DIRECTION DES RESSOURCES HUMAINES, DU DÉVELOPPEMENT ORGANISATIONNEL ET DES AFFAIRES JURIDIQUES (DRHDO-AJ)

- Assure que l'information portant sur la présente politique est intégrée dans le cursus de la journée de bienvenue des nouveaux employés ;

- Conseille et soutient les gestionnaires dans l'application des mesures administratives ou disciplinaires, au besoin.

6.6 UTILISATEUR

- Responsable de se conformer aux règles et mesures de sécurité de la présente politique ;
- Responsable des données acheminées et reçues ;
- Assure de maintenir le niveau de sécurité d'accès à l'information selon ses responsabilités ou fonctions dans l'organisation ;
- Avise son supérieur/répondant ainsi que le responsable de la sécurité de la DRIM lors d'une possible faille de sécurité.

7 OBLIGATIONS

7.1 OBLIGATIONS GÉNÉRALES

7.1.1 Privilège d'utilisation

Les directeurs et gestionnaires sont responsables d'accorder à leur personnel le privilège d'utiliser les ressources informationnelles qui sont sous la responsabilité de la DRIM. Chaque utilisateur est responsable d'accéder uniquement aux ressources informationnelles nécessaires à l'exécution normale de son travail.

Ce privilège est susceptible d'être révoqué en tout temps pour cause, et ce, en conformité avec la présente directive et les lignes directrices internes de l'organisation ou de la DRIM.

7.1.2 Utilisation éthique des ressources informationnelles

En plus de se conformer aux règles éthiques propres à l'organisation, toute personne visée par la présente politique **doit suivre les règles d'utilisation éthique** des ressources informationnelles visées par cette politique :

1. Il est interdit de télécharger, partager, copier, installer ou exécuter tout logiciel sur une ressource informationnelle visée par cette politique, sans une approbation préalable de la DRIM ;
2. Il est interdit d'utiliser à son profit les ressources informationnelles ;
3. Il est interdit d'interconnecter des équipements non approuvés à des ressources informationnelles ;
4. Il est interdit de créer, expédier ou réexpédier tout courriel, message ou fichier qui est susceptible d'affecter le fonctionnement ;
5. Il est interdit de partager ses identifiants et ses mots de passe ;
6. Il est interdit de désactiver ou modifier les mécanismes de protection en vigueur.

7.1.3 Gestion des identités et des accès

Chaque utilisateur est responsable de ses identifiants ainsi que de ses mots de passe. Il a l'obligation de les protéger et de ne pas les divulguer. Pour toutes les ressources logicielles, l'ensemble des utilisateurs doit se conformer aux modalités en vigueur lors de sa demande d'accès, qui doit être approuvée par un gestionnaire ou toutes autres personnes désignées.

7.1.4 Utilisation de l'Internet

Respecter les règles d'utilisation de l'Internet :

1. Il est interdit d'utiliser les outils d'accès à l'Internet ou le réseau de télécommunication du réseau la santé pour propager quelques virus ou toute forme de cyberattaque que ce soit sur les réseaux d'information de l'organisation ou tout autre réseau externe ;
2. Il est interdit de rendre inutilisable ou surcharger l'ordinateur ou le réseau utilisé ;
3. Il est interdit de contourner tout système mis en place pour protéger la vie privée ou la sécurité des utilisateurs ;
4. Il est interdit de télécharger ou distribuer des données ou des logiciels piratés ;
5. Il est interdit de naviguer sur des sites réputés malveillants (Dark Web) ;
6. Il est interdit d'afficher, d'archiver, d'enregistrer, de distribuer ou d'éditer des documents ou des graphiques sexuellement explicites, haineux ou racistes sur les réseaux d'information de l'organisation ;
7. Il est interdit de naviguer sur des sites Internet à des fins personnelles ;
8. Respecter le droit d'auteur des logiciels, des informations et de la documentation utilisée ;
9. Faire preuve de prudence et de vigilance sur sa navigation Internet afin de ne pas télécharger du matériel potentiellement dangereux ; l'utilisateur ayant des droits d'accès à haut privilège demeure responsable de tout téléchargement qu'il effectue sur les ressources informationnelles de l'établissement.

7.1.5 Utilisation des Médias sociaux

En plus de respecter les règles énumérées précédemment, l'utilisateur doit suivre les directives et recommandations de la politique d'utilisation des médias sociaux de l'établissement.

7.1.6 Utilisation du système de courriel électronique

1. L'utilisation du courriel électronique est réservée à des fins professionnelles ;
2. Tout contenu produit à l'aide du courrier électronique de l'organisation demeure la propriété de l'organisation ;
3. L'utilisateur est responsable du contenu des messages envoyés et reçus ;
4. En plus de respecter les responsabilités générales d'utilisation énumérées précédemment, l'utilisateur doit se référer à la rubrique sur les conditions d'utilisation Outlook du MSSS (MSSS Outils de collaboration Suite Office 365 « Termes et conditions d'utilisation des outils de collaboration »).

7.1.7 Utilisation des outils collaboratifs infonuagiques fournis par le MSSS

1. Toute personne visée par la présente politique et ayant accès aux outils de collaboration doit suivre les recommandations du MSSS pour l'utilisation éthique et sécuritaire des outils collaboratifs incluant le système de messagerie provincial (Outlook), mis à la disposition des utilisateurs du RSSS (voir les « *Termes et conditions d'utilisation des outils de collaboration* », disponible sur la plateforme en ligne) ;
2. Les outils de collaboration offerts par le MSSS répondent aux exigences ministérielles et gouvernementales de sécurité de l'information, sauf dans les cas où le MSSS aurait explicitement mentionné autrement ; les utilisateurs sont tenus

d'utiliser, dans le cadre de leurs fonctions, les outils de collaboration fournis par le MSSS et d'en adopter un usage exemplaire, au regard des dispositions du cadre de gouvernance de la sécurité de l'information et des meilleures pratiques en la matière ;

3. Les outils de collaboration ne doivent aucunement se substituer aux processus d'affaires en place, ils viennent compléter l'offre de service ministérielle en matière de technologie de l'information ; les systèmes d'information en place doivent donc être utilisés en priorité lorsqu'ils sont disponibles ;
4. Tout contenu produit à l'aide des outils de l'organisation demeure la propriété de l'organisation.

7.1.8 Règles sur le télétravail et la télésanté

Les utilisateurs doivent respecter et se conformer aux règles en vigueur sur le télétravail et la télésanté énoncées dans les différentes politiques de l'organisation et dans les directives sur la télésanté du MSSS, afin d'assurer la sécurité des ressources informationnelles utilisées.

7.2 OBLIGATIONS SPÉCIFIQUES

7.2.1 Pour tous les utilisateurs

Chaque utilisateur des ressources informationnelles de l'organisation est responsable :

1. De respecter en tout temps la présente politique et les documents d'encadrement en sécurité des ressources informationnelles en vigueur ;
2. De s'assurer de bien procéder à une fermeture de session ou un verrouillage de son poste de travail lorsque ses tâches sont terminées, ou lorsqu'il s'absente de son poste de travail ;
3. De changer son mot de passe selon les modalités en vigueur ;
4. De **signaler dans les plus brefs délais** au Centre d'assistance informatique de la DRIM le vol ou la perte d'une ressource informationnelle (ex. : appareil mobile, portable, etc.) ;
5. De **signaler dans les plus brefs délais** au Centre d'assistance informatique de la DRIM, selon les modalités en vigueur, tout événement lié à la sécurité des ressources informationnelles ayant comme impact de compromettre les activités de son service, sa direction, son département ou de l'organisation ;

   Exemple où l'intégrité et la disponibilité des ressources informationnelles sont compromises : à l'ouverture d'un courriel avec un hyperlien ou une pièce jointe suspecte qui a générée l'infection et provoque un comportement non habituel de son ordinateur.

Pour les équipements connectés/via les ressources informationnelles, mais non sous la responsabilité de la DRIM, vous devez vous adresser au service de l'établissement qui est responsable de fournir de l'assistance (ex. : caméras de surveillance, équipements GBM, etc.).

7.2.2 Pour les gestionnaires

Tout gestionnaire est responsable de l'application et du respect de la présente politique au sein de son service ou de son unité administrative, de même que de l'application

des directives touchant la sécurité et de bonnes pratiques en cette matière. Notamment, le gestionnaire doit :

1. Sensibiliser les membres de son personnel à la protection des ressources informationnelles, aux conséquences d'une atteinte à la sécurité ainsi qu'à leurs responsabilités en la matière ;
2. Veiller à ce que les employés sous sa gouverne utilisent correctement les ressources informationnelles ;
3. Voir également à inclure dans les contrats et les ententes ; les clauses sur la sécurité des ressources informationnelles.

7.2.3 Pour les tiers et les fournisseurs

Les tiers et les fournisseurs ayant accès aux ressources informationnelles doivent respecter la présente politique et les exigences de sécurité de la direction de ressources informationnelles de la Montérégie.

8 MODALITÉS D'APPLICATION OU PROCÉDURE

8.1 MESURES DE CONTRÔLE

Plusieurs mesures de contrôle sont en place afin de garantir une protection des ressources informationnelles face aux erreurs de manipulation, pannes de systèmes informatiques, à la propagation des virus et des cyberattaques.

Les mesures de contrôle additionnelles exigées par le MSSS notamment, dans sa règle particulière sur la sécurité organisationnelle (RPSO) font l'objet d'un plan d'action annuel et d'un bilan annuel au MSSS.

8.2 DROIT DE REGARD

En conformité avec la législation et la réglementation en vigueur, la DRIM se réserve le droit de surveiller et d'auditer les ressources matérielles et logicielles, ainsi que tout usage des ressources informationnelles de l'organisation visées par cette politique. Ceci ayant au préalable été autorisé par la DRHDO-AJ pour les employés, la direction des services professionnels pour les médecins ou encore des directions responsables des contrats de services octroyés à des tiers.

Des mécanismes de surveillance sont en place afin de permettre à la DRIM de démontrer la conformité de cette politique aux CISSS de la Montérégie et au ministère de la Santé et des Services sociaux.

8.3 SANCTIONS

Tout membre du personnel ou toute tierce partie autorisée qui contrevient à la présente politique s'expose selon les circonstances et la gravité de son geste, à des pénalités prévues aux différentes législations, conventions collectives, ententes ou contrats, notamment à :

- Des mesures disciplinaires ou administratives pouvant aller jusqu'au congédiement ou à la fin d'une entente ou d'un contrat, selon les politiques en vigueur au sein de l'organisation ;

- Au retrait de certains droits d'accès aux équipements et aux services visés par la présente politique ;
- Aux sanctions pénales qui pourraient s'appliquer selon le cas et prévues par une loi (exemple : la LPCRS qui encadre le Dossier Santé Québec).

9 DISPOSITIONS FINALES ET TRANSITOIRES

La présente politique de sécurité des ressources informationnelles entre en vigueur dès son adoption.

10 RÉVISION

Cette politique doit être révisée aux trois (3) ans ou à l'occasion de changements organisationnels ou de nouvelles orientations ministérielles, afin d'intégrer les nouveaux besoins, les nouvelles pratiques, les nouvelles menaces et les nouveaux risques encourus.

11 RÉFÉRENCES

HISTORIQUE DES VERSIONS (du plus ancien au plus récent)		
Numéro et titre	**Date d'adoption**	**Établissement d'origine**
DRIM-101 Politique de sécurité des ressources informationnelles	2022-09-22	CISSSMC

RÉDIGÉE OU RÉVISÉE PAR **Équipe Sécurité, Direction des ressources informationnelles de la Montérégie**
PERSONNES CONSULTÉES Chantal Normandeau, Directrice régionale des ressources informationnelles de la Montérégie L'ensemble des gestionnaires de la Direction des ressources informationnelles de la Montérégie