Centre intégré universitaire de santé et de services sociaux de l'Est-de-l'Île-de-Montréal
Québec

Direction des ressources technologiques

POLITIQUE

GESTION DES ACCÈS AUX SYSTÈMES D'INFORMATION ET SESSION UTILISATEUR		
Nº Politique : **POL-058**	Responsable de l'application : Direction des ressources technologiques	
Nº Procédure découlant : **s.o.**		
Approuvée par : **Comité de direction**	Date d'approbation : **2024-06-11**	Date de révision : **2028-06-11**
Destinataires : Toute personne physique ou morale qui, à titre d'employé, de consultant, de partenaire ou de fournisseur, utilise les actifs informationnels du CIUSSS-EMTL ou y a accès.		

1. CONTEXTE

Avec l'utilisation grandissante des systèmes d'information dans le domaine de la santé et des services sociaux, les établissements du réseau de la santé ont l'obligation de mettre en place un mécanisme de gestion d'accès aux systèmes d'information.

Cette même obligation est également énoncée à la section 7 de la règle particulière sur la sécurité organisationnelle[1]. Le CIUSSS de l'Est-de-l'Île-de-Montréal (CIUSSS-EMTL), pour répondre aux exigences de conformité du ministère de la Santé et des Services sociaux (MSSS), a mis en place un mécanisme de gestion des accès centré sur les bonnes pratiques du réseau de la santé et des services sociaux.

2. CHAMP D'APPLICATION

La présente politique s'applique aux utilisateurs d'actifs informationnels, c'est-à-dire à toute personne oeuvrant au sein du CIUSSS-EMTL, de quelque catégorie d'emploi et de statut d'employé que ce soit, les médecins, les médecins résidents, les dentistes, les pharmaciens, les chercheurs, le personnel de soins et services, administratif ou de soutien, les pairs aidants, les stagiaires, les bénévoles, ainsi que toute personne physique ou morale qui, par engagement contractuel ou autrement, utilise un actif informationnel du CIUSSS-EMTL ou y a accès.

L'information visée est celle que le CIUSSS-EMTL détient dans l'exercice de ses fonctions, que sa conservation soit assurée par lui-même ou par un tiers, incluant entre autres, les informations sur les usagers ou les employés, les documents administratifs ou professionnels.

[1] *Mise en oeuvre de la règle particulière sur la sécurité organisationnelle, MSSS-GUI02, 14 avril 2016*

3. OBJECTIFS[2]

Le processus de gestion des accès vise, principalement, à assurer la confidentialité et l'intégrité du système d'information, contribuant ainsi à sa sécurité.
La mise en place d'un processus de gestion des accès permet, notamment de:

- Octroyer les bonnes autorisations à des personnes sur les bonnes ressources ;
- Renforcer la sécurité de l'information de l'organisation en garantissant la cohérence d'attribution des droits d'accès aux ressources hétérogènes du système d'information ;
- Répondre aux exigences légales et réglementaires;
- Mettre en place les structures de gouvernance pour une saine gestion des accès aux actifs informationnels ;
- Assurer une traçabilité des accès aux systèmes d'information ;
- Se servir d'éléments probants lors de la conduite d'enquête, advenant un incident.

4. DÉFINITIONS

4.1. Actif informationnel

Un actif informationnel est soit une banque d'information, un système d'information, un réseau de télécommunication, une infrastructure technologique ou un ensemble de ces éléments, ainsi qu'une composante informatique d'un équipement médical spécialisé ou ultraspécialisé[3].

Un actif informationnel inclut tout document constitué d'information portée par un support papier ou tout type de support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles sous l'une de ces formes ou en un autre système de symboles[4].

4.2. Autorisation

Selon la définition du document Règle Particulière sur la Sécurité Organisationnelle (RPSO) du MSSS datant d'avril 2016, l'autorisation est une procédure qui consiste à octroyer des privilèges d'accès à un utilisateur selon des règles bien précises.

4.3. Compte utilisateur standard

Un compte utilisateur standard permet d'utiliser la plupart des fonctionnalités du système d'information. Le niveau de sécurité est déterminé par le détenteur et octroyé par le pilote de l'actif informationnel (englobant les systèmes d'information et les bases de données). Le principe de moindre privilège doit être soumis à chaque utilisateur standard.

---

[2] *Guide de gestion des accès à l'information, MSSS-GUI07, 01-05-2017*
[3] *Loi concernant le partage de certains renseignements de santé,* RLRQ c P-9.0-001, art 3 (1◦)
[4] *Loi concernant le cadre juridique des technologies de l'information, RLRQ c C-1., art 3.*

4.4. Compte administrateur

4.4.1. Compte administrateur local

Un compte administrateur local peut non seulement avoir les mêmes privilèges qu'un compte standard, mais il peut aussi servir de compte de service local à l'ordinateur. Ce compte est autorisé à agir sur la totalité du système d'exploitation, et ainsi pouvoir définir des paramètres communs à tous les utilisateurs. Un compte administrateur local peut aussi exécuter des logiciels, même si ceux-ci proviennent de sources douteuses.

Un compte administrateur local a un niveau de privilège qui est limité à l'équipement. Son rayon d'action se limite à l'équipement pour lequel il a été créé.

4.4.2. Compte administrateur de domaine

Ce compte est réservé aux administrateurs systèmes faisant partie de la Direction des ressources technologiques (DRT). Leur rayon d'action est presque illimité et c'est pour cette raison que l'administrateur système ne l'utilise que pour des tâches spécifiques. Chaque intervention avec ce compte est journalisée et documentée par l'administrateur.

4.5. Compte de service

Un compte de service est un compte créé explicitement afin de fournir un contexte de sécurité pour les services exécutés. Le contexte de sécurité détermine la capacité du service pour accéder au domaine local, aux ressources réseaux. Son rayon d'action se limite au service dans le domaine ou à un équipement spécifique.

4.6. Détenteur de l'information[5]

Employés désignés par le dirigeant du CIUSSS-EMTL ou son délégué, appartenant à la classe d'emploi de niveau cadre et dont le rôle est, entre autres, de s'assurer de la sécurité de l'information et des ressources qui la sous-tendent, relevant de la responsabilité de leurs unités administratives.

4.7. Code d'utilisateur

Moyen par lequel un utilisateur fournit une identité réclamée par le système. L'identifiant permettra au système d'accorder un niveau d'accès.

4.8. Privilège d'accès

Ces accès accordent à l'utilisateur certaines autorisations ou permissions supplémentaires.

[5] *Directive sur la sécurité de l'information gouvernementale, Secrétariat du Conseil du trésor, 15 janvier 2014.*

4.9. Principe de moindre privilège[6]

Le principe du privilège minimal exige que l'utilisateur ne dispose pas de plus de droits que nécessaire pour accomplir ses tâches. Cela implique que les autorisations accordées à un rôle constituent le strict minimum nécessaire à l'accomplissement des tâches associées à ce rôle.

4.10. Authentication unique [Single Sign-On (SSO)]

La méthode d'authentification unique permet à un utilisateur de se connecter à plusieurs applications ou services d'un simple clic à l'aide d'un service comme l'active directory récupérant l'identifiant et le mot de passe de l'utilisateur.

4.11. Système d'information[7]

Système constitué des Ressources humaines (le personnel), des Ressources matérielles (l'équipement) et des procédures permettant d'acquérir, de stocker, de traiter et de diffuser les éléments d'information pertinents pour le fonctionnement d'une entreprise ou d'une organisation.

5. ÉNONCÉ

Tout actif informationnel (système d'information, application ou autre) doit avoir un détenteur qui en fixe les règles et modalités d'accès.

5.1. La gestion des droits d'accès basée sur les rôles où l'appartenance à un groupe est privilégiée

Le but de ce modèle est de donner accès à une personne, ou à un groupe ayant la même fonction, aux mêmes privilèges d'accès. Le rôle est dans la plupart des cas déterminé par les tâches confiées à l'utilisateur dans l'exercice de ses fonctions.

5.2. Principe de séparation des tâches

Principe de sécurité selon lequel les responsabilités liées à une activité de nature sensible sont réparties entre plusieurs entités (personnes, processus, etc.) afin d'éviter qu'une seule entité n'exerce un contrôle sur l'ensemble de l'activité. Il vise à limiter les possibilités d'abus et d'infraction par une seule personne.
Exemple : une personne ne doit pas avoir la possibilité de commander une fourniture ou une prestation et celle de valider sa réception.

[6] Guide de gestion des accès logiques : réalisée par le Sous-secrétariat du dirigeant principal de l'information et produite en collaboration avec la Direction des communications, en novembre 2016.
[7] Cadre de gestion de la sécurité de l'information du CIUSSS-EMTL

5.3. La gestion du mot de passe et des accès

La gestion du mot de passe doit respecter les principes suivants :

- Sauf exception, tout mot de passe émis par le CIUSSS-EMTL doit être temporaire (il ne faut jamais activer l'option où le mot de passe n'expire jamais pour un compte utilisateur);
- L'utilisateur doit lui-même choisir son mot de passe;
- L'utilisation d'un dispositif de lecture vocale de mot de passe est strictement interdite;
- Imposer l'utilisation d'un mot de passe respectant les règles de complexité :
    - Faire expirer un mot de passe après un délai déterminé ou lorsque survient un changement chez des utilisateurs disposant du mot de passe d'un compte partagé;
    - Rendre impossible la réutilisation des derniers mots de passe :
        - Respecter les modalités de gestion relatives à la saisie infructueuse du mot de passe et à sa modification en cas de perte ou d'oubli.

La création d'un compte, il est impératif de respecter la politique de gestion de mot de passe fournissant les mesures pour assurer adéquatement la sécurité des accès aux actifs.

∗ ***Exception***
Seuls les comptes de service et certains comptes doivent avoir l'option « le mot de passe n'expire jamais ».

Un registre des comptes de service doit être tenu et mis à jour par le chef de service infrastructure.

5.4. Ne jamais accorder de comptes génériques sauf exception

À l'embauche, l'établissement doit attribuer au nouvel employé un code unique qui lui permettra de s'authentifier pour accéder aux ressources et accomplir sa fonction. Ce compte, qui est une combinaison d'un code d'utilisateur et d'un mot de passe, permettra au système de l'établissement d'attribuer les accès auxquels l'utilisateur a droit.

Les comptes génériques sont des comptes partagés qui sont utilisés par plusieurs utilisateurs afin d'accéder à des ressources ou effectuer des tâches très spécifiques. Bien que leur utilisation puisse parfois être nécessaire, nous limiterons au maximum la création de ce type de compte, car il est difficile de retracer les actions d'une personne précise à partir de ce type de compte. Des cas d'exception peuvent être demandés sous approbation et chaque compte générique sera répertorié dans un registre.

Pour les comptes génériques, puisqu'ils ne sont liés à aucune personne physique ni morale, le système n'a aucun moyen d'identifier l'auteur des modifications. Un

utilisateur avec un compte générique peut exécuter les mêmes tâches qu'un utilisateur normal, sans que le système puisse l'identifier, ce qui compromet la confidentialité et l'intégrité du système.

Exemple : Dans le cas d'un accès à une application clinique, si un compte générique est utilisé pour ouvrir l'ordinateur, le seul périmètre de sécurité qui reste à notre système est l'authentification de l'application. Et nous pouvons noter dans ce cas que plus le temps de verrouillage est long, plus le système est à risque (ANNEXE 2).

Chaque direction détentrice d'un système d'information est tenue de maintenir un registre des comptes génériques qui sont sous sa supervision. Il est également de sa responsabilité de retirer tous les utilisateurs inactifs après un certain délai.

Un audit de l'utilisation de ces comptes peut être demandé à tout moment par le chef de la sécurité de l'information organisationnelle (CSIO) pour s'assurer de l'utilisation adéquate de ces comptes.

Un compte générique doit uniquement avoir des droits minimums. En aucun cas, il ne peut recevoir des accès privilèges.

∗ ***Exceptions et mesures prises :***

Pour pouvoir gérer efficacement ces comptes génériques, les règles suivantes sont à respecter :

- La demande du code générique doit être approuvée par le détenteur de l'application ou un cadre supérieur du secteur ;
- Une configuration personnalisée sera faite sur l'ordinateur pour permettre à l'utilisateur de ne disposer que du strict minimum (simplement les accès qui lui permettront d'accomplir ses tâches) ;
- Le compte générique ne pourra pas accéder à Internet afin de diminuer le risque d'une infection virale ;
- Le compte générique ne pourra pas accéder au répertoire réseau de l'établissement ;
- Le gestionnaire de l'utilisateur doit demander la suppression du compte auprès du détenteur du système d'information, si l'utilisateur n'en trouve plus l'utilité ;
- Une fois créé, le compte générique est sous la responsabilité de la direction qui en a fait la demande ;
- Le responsable s'assure de vérifier la liste des utilisateurs dans les comptes génériques et de les retirer dès que nécessaire ;
- Un compte générique ne doit jamais avoir des privilèges d'administrateur local d'un poste.

5.5. Les privilèges d'administrateur

Donner des privilèges d'administrateur à un utilisateur lui octroie des droits spéciaux comme la capacité d'installer des logiciels, de modifier des configurations critiques ou encore de supprimer ou créer des accès.

Les pirates informatiques s'intéressent beaucoup à ce type de compte, car s'ils réussissent à obtenir ces droits, alors ils pourront agir ce qui aura des conséquences graves pour l'organisation.

Cependant, dans certains cas, il est nécessaire que des utilisateurs puissent avoir accès à ces droits afin de maintenir des actifs informationnels qui nécessitent des privilèges d'administrateur, par exemple.

Si l'utilisateur veut avoir ce type de privilèges, il doit en faire la demande auprès de la Direction des ressources technologiques (DRT). La demande doit d'abord être approuvée par son directeur ou son directeur adjoint avant d'être traitée, et par la suite une analyse du contexte sera effectuée par les personnes en charge de la sécurité.

Chaque direction est tenue de maintenir un registre des comptes administrateurs qui sont sous sa supervision.

5.6. Révoquer les privilèges d'accès des membres du personnel dès leur fin d'emploi

Afin d'assurer la sécurité de l'information, à la fin de son mandat ou à la fin de son emploi (retraite, congédiement, etc.), la Direction des ressources humaines (DRH) doit communiquer avec la DRT pour un retrait de tous les accès dont la personne bénéficiait.

Pour éviter les contraintes liées aux délais de traitement, il est conseillé de faire la demande avant le départ de l'utilisateur en spécifiant la date exacte de son départ. Pour pouvoir gérer la continuité des tâches que l'employé avait en charge, le supérieur immédiat peut faire une demande de sauvegarde des documents de l'utilisateur avant la suppression définitive du compte.

Dans le cas où l'utilisateur n'est pas dans les registres de la DRH, par exemple les médecins, les stagiaires ou les chercheurs, le gestionnaire en charge de l'utilisateur doit s'assurer qu'une demande de retrait des accès est envoyée au pilote des systèmes d'information.

Chaque direction est responsable de retirer les accès des utilisateurs venant des solutions infonuagiques d'un tiers.

Un utilisateur ne faisant plus partie de l'organisation peut encore avoir accès à certaines solutions infonuagiques si l'option d'authentification par SSO n'est pas activée.

5.7. Restreindre des privilèges d'accès Internet à des tiers

Les privilèges d'accès Internet pour un tiers ne doivent pas être accordés, à moins que le supérieur hiérarchique ou le gestionnaire responsable de l'utilisateur ne confirme qu'il s'agit d'un besoin professionnel valable. Ces accès ne doivent être activés que pour les personnes concernées, et seulement pour la période nécessaire au travail autorisé.

5.8. Les comptes des tiers doivent rester désactivés, sauf exception

Le compte attribué à un tiers doit rester désactivé en tout temps. Pour que le compte soit réactivé, le fournisseur doit faire une demande et justifier son intervention dans la demande. Il doit aussi donner le temps que prendra son intervention et la date de l'intervention.

Par rapport à ces informations, l'intervenant de la DRT réactivera le compte avec une date d'expiration.

* ***Exception***

  Si le compte doit rester actif, par exemple un compte de service qui communique avec un serveur distant, cette option doit être précisée dès la demande de création du compte. Le nom du responsable de ce compte chez le fournisseur doit être obtenu.
  Les droits d'un compte de service doivent se limiter uniquement aux tâches pour lesquelles il a été créé.

5.9. Désactiver les comptes après une période de trois mois d'inactivité

Cette partie concerne les comptes utilisateurs inactifs depuis plus de trois mois et qu'aucune information les concernant n'a été enregistrée.

Les droits d'accès sont révisés par la DRT toutes les six semaines. La DRT est chargée de suspendre tout compte utilisateur inactif depuis plus trois mois. Si au bout d'un an le propriétaire de ce compte ne se manifeste pas, le pilote ou l'administrateur doit supprimer le compte[8].

Il faut noter aussi que tout compte utilisateur inactif pendant une année sera immédiatement supprimé.

5.10. Suppression de documents numériques du répertoire personnel de l'utilisateur après le départ d'un employé

Étant donné que les sauvegardes annuelles et mensuelles sont déjà conservées et renferment déjà les dossiers de l'utilisateur, il n'est pas pertinent de garder les fichiers de l'utilisateur qui n'est plus en poste.

[8] 64 mesures obligatoires du CGGAI – Volet sécurité, extrait de la CGGAI appartenant aux organismes du réseau de la santé et des services sociaux V2007-03-12 (représente toujours une référence de bonne pratique)

Le répertoire personnel d'un utilisateur va être conservé pour une durée à déterminer avec la direction. Sauf avis contraire du gestionnaire, les répertoires de l'utilisateur seront supprimés après ce délai.

Pour les comptes désactivés depuis une période de plus de trois mois, les fichiers dans les répertoires personnels d'un ancien utilisateur sont supprimés au même moment que le compte utilisateur.

Pour la continuité du service, un gestionnaire peut demander le transfert des documents de travail pour le ou la remplaçant(e).

5.11. Révision régulière des droits d'accès ou des privilèges d'un utilisateur

Les privilèges d'accès aux systèmes d'information, accordés à tous les utilisateurs, doivent être réévalués annuellement par le supérieur immédiat de chaque utilisateur[9]. Cette révision sert entre autres à déterminer si les privilèges accordés correspondent toujours aux besoins de l'utilisateur dans le cadre de son travail.

Le départ, le transfert ou la mutation d'un utilisateur ainsi que tout autre changement relatif à ses tâches et ses fonctions doit conduire systématiquement à la révision de ses droits d'accès et de respecter le principe du moindre privilège, c'est-à-dire, qu'ils ne doivent avoir ni plus, ni moins comme accès.
Le gestionnaire responsable doit s'assurer que les droits attribués à l'utilisateur répondent toujours aux besoins de celui-ci.

Afin d'assurer la sécurité de l'information, si un utilisateur change de fonction, tous ses accès doivent être révisés et approuvés par les supérieurs immédiats concernés.

Ainsi, les détenteurs pourront faire une correction dans les privilèges de l'utilisateur et éviter d'avoir des privilèges qui ne sont plus d'actualité.

Il est fortement déconseillé de copier-coller un profil d'un autre utilisateur quand celui intègre l'organisation ou change de rôle.

5.12. La gestion des comptes de services

Les comptes de services doivent être enregistrés dans un registre avec un accès très restreint. La responsabilité de gestion et de mise à jour de ce registre appartient à la DRT.

[9] Guide de gestion des accès à l'information, MSSS-GUI07, 1ER mai 2017.

6. RÔLES ET RESPONSABILITÉS

6.1. Détenteur de l'information[10]

Les détenteurs sont responsables des actifs informationnels qui leur sont confiés. Les détenteurs de l'information, ou leurs délégués, doivent s'assurer de la sécurité de l'information, incluant les ressources qui la sous-tendent (humaines, matérielles et financières), notamment de :

- Nommer les pilotes pour les systèmes d'information dont ils ont la responsabilité ;
- Catégoriser l'information[11] relevant de leur responsabilité en matière de disponibilité (D), d'intégrité (I) et de confidentialité (C) ;
- Agir comme maîtres d'oeuvre des analyses de risques de sécurité de l'information et de la détermination du niveau de protection requis ;
- S'assurer de l'élaboration des contrôles non technologiques et de la prise en charge des risques résiduels de sécurité ;
- Déterminer ou valider les règles d'accès aux actifs informationnels sous leur responsabilité ;
- Participer au besoin à l'élaboration des orientations stratégiques, des politiques, des directives, des cadres de gestion, des guides, des plans d'action et des bilans ;
- S'assurer de l'élaboration, de l'approbation, de la mise en place et de l'application des mesures de sécurité de l'information pour les actifs informationnels (tous supports confondus) dont ils ont la charge, en partenariat avec la Direction des ressources technologiques pour le volet technologique; ces mesures incluent celles liées au respect des exigences légales de protection des renseignements personnels ;
- Établir et maintenir à jour le plan de relève des systèmes d'information dont ils sont détenteurs, en collaboration avec les partenaires concernés ;
- S'assurer de l'adéquation des mesures de sécurité de l'information en vigueur par rapport aux risques encourus, en partenariat avec la DRT pour le volet technologique ;
- Participer à l'établissement et à la mise à jour du plan de continuité des services, en collaboration avec les partenaires concernés.

6.2. Pilote d'application

Le pilote de l'application a la responsabilité de :

- S'assurer de respecter la présente politique de gestion des accès ;
- Gérer le niveau d'accès attribué à un utilisateur à la demande du supérieur immédiat de l'utilisateur ;
- Déterminer ou participer au besoin à la détermination des règles d'accès aux actifs informationnels sous leur responsabilité, et les faire valider par le détenteur de l'information; assurer la gestion de ces règles d'accès ;

[10] Cadre de gestion de la sécurité de l'information du CIUSSS-EMTL

[11] Cette même valeur de catégorisation se retrouvera aussi dans le calendrier de conservation du CIUSSS-EMTL (cote DIC), où elle doit également être déterminée par les détenteurs de l'information selon le Recueil des règles de conservation des documents des établissements de santé et de services sociaux / Version 1.4, 2017, section A, paragraphe 6.

- Donner ou révoquer les droits à la demande du supérieur immédiat de l'employé ;
- Mettre à jour le profil d'accès d'un utilisateur, sur demande du supérieur immédiat ;
- S'assurer de la modification des privilèges et des droits d'accès suite aux mouvements des utilisateurs (changement de statut, de fonction ou départ) qui leur sont communiqués par la procédure de modification de profil ;
- Soumettre au détenteur l'état de la situation en rapport avec les autorisations d'accès.

6.3. Chef de la sécurité de l'information organisationnelle (CSIO)

Le CSIO est chargé de :

- Élaborer et mettre à jour la présente politique et de la soumettre pour validation au comité de sécurité de l'information ;
- Soumettre à l'approbation du comité de sécurité de l'information, la présente politique et d'assurer le suivi de sa mise en oeuvre. Il lui soumet également toute dérogation à l'application de la politique ;
- Définir et mettre en oeuvre le processus de gestion des accès à l'information;
- S'assurer de la documentation et de la mise à jour des procédures nécessaires à la mise en place du processus de gestion des accès et d'assurer le suivi de sa mise en œuvre ;
- Réaliser, périodiquement, un audit des mécanismes de contrôle de gestion des accès.

6.4. Coordonnateur organisationnel des mesures de sécurité (COMSI)

Le COMSI collabore étroitement avec le CSIO et lui fournit le soutien nécessaire à l'exercice de ses responsabilités en matière de gestion des accès. À ce titre, il :

- Contribue à l'élaboration, la mise en oeuvre et la révision de la politique de gestion des accès ;
- Contribue à l'élaboration et à la mise en oeuvre du processus de gestion des accès ;
- Détermine les menaces et les situations de vulnérabilité liées à la gestion des accès et, si requis, propose des mesures de renforcement des contrôles des accès ;
- S'assure, périodiquement, auprès des détenteurs et du responsable des technologies de l'information, que les profils d'accès ainsi que les autorisations consignées aux matrices sont conformes et à jour ;
- Formule des avis de pertinence sur les mécanismes de gestion des accès mis en place ;
- À la demande du CSIO, produit un audit annuel des droits attribués aux différents groupes et utilisateurs des systèmes d'information.

6.5. Comité de sécurité de l'information

Le comité de sécurité de l'information :

- Contribue à l'élaboration, la mise en œuvre et la révision de la politique de gestion des accès ;
- Recommande l'adoption de la politique de gestion des accès et en assure la diffusion ;
- Recommande toute dérogation aux dispositions de la politique de gestion des accès ;
- S'assure que les gestionnaires des unités administratives définissent et mettent à jour les autorisations et les critères d'autorisation correspondant à chaque rôle relevant de leur autorité ;
- S'assure que les détenteurs de l'information sont désignés et assument pleinement leurs responsabilités en matière de gestion des accès ;
- S'assure que les détenteurs de processus documentent clairement les processus relevant de leur autorité et particulièrement, les règles de séparation de tâches ;
- S'assure que les gestionnaires révisent, périodiquement, les autorisations d'accès octroyées à leurs employés.

6.6. La Direction des ressources technologiques (DRT)

La Direction des ressources technologiques a la responsabilité de :

- Donner ou révoquer des comptes utilisateurs ;
- Augmenter ou restreindre des privilèges d'accès dans le réseau, à la demande du supérieur immédiat de l'utilisateur ;
- Assurer la vérification régulière des droits des différents partages réseaux et faire mention de toute anomalie au responsable de la sécurité ;
- S'assurer que les fournisseurs respectent ces exigences ;
- S'assurer de la mise en place et la vérification des journaux pour les systèmes d'information sous sa responsabilité ;
- S'assurer de la mise en place des stratégies de gestion d'accès des systèmes d'information sous sa responsabilité.

6.7. Les gestionnaires

Les gestionnaires de la direction :

- S'assurent de la conformité des qualifications de leur personnel aux critères d'autorisation associés à leurs rôles ;
- S'assurent de la compréhension et de l'application de la présente politique de gestion des accès par leurs employés ;
- Remplissent les formulaires[12] nécessaires à la gestion des identifiants et des autorisations d'accès lors de l'entrée en fonction d'un utilisateur, de son affectation, de son départ ou de son absence prolongée ;

[12] Ces formulaires sont disponibles dans l'outil de gestion des requêtes (Octopus).

- Révisent, périodiquement, les autorisations d'accès attribuées à leurs utilisateurs et veillent à leur conformité aux autorisations associées aux postes de travail occupés ;
- Gèrent les exceptions d'accès attribuées et s'assurent de leur retrait lorsque non requises ;
- S'assurent que les autorisations et les critères d'autorisation définis sont conformes aux descriptions de tâches des processus métiers et aux profils d'accès définis dans les matrices des profils d'accès ;
- Signalent au détenteur toutes modifications des autorisations ou des critères d'autorisation associées aux rôles sous sa responsabilité.

Le supérieur immédiat ou le cadre supérieur est responsable des comptes génériques dont il a fait la demande.

7. ÉLABORATION, RÉDACTION ET MISE À JOUR DE LA POLITIQUE

7.1. Chef de la sécurité de l'information organisationnelle (CSIO)

Le CSIO est responsable de l'élaboration, de la rédaction et de la mise à jour de la politique, en collaboration avec la Direction des Ressources Technologiques.

7.2. Comité de sécurité de l'information

Les membres du comité de sécurité de l'information ont participé à la validation de la politique et participent à la validation de sa mise à jour.

7.3. Calendrier de révision de la politique

La présente politique devra être révisée tous les 4 ans ou plus rapidement en fonction des besoins.

8. RESPONSABLE DE LA MISE EN APPLICATION

8.1. Chef de la sécurité de l'information organisationnelle (CSIO)

Il est responsable de la mise en application de la présente politique.

9. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur le jour de son adoption par le Comité de direction et annule, par le fait même, toute autre politique en cette matière adoptée antérieurement dans l'une ou l'autre des installations administrées par le CIUSSS-EMTL.

10. ANNEXE

ANNEXE 1 – *Stratégie de gestion des comptes Windows*

ANNEXE 2 – *Périmètre de sécurité pour l'accès à l'information*

ANNEXE 1 : Stratégie de gestion des comptes Windows

Option Windows[13]	***Description***	***Valeur***
Durée de verrouillage de compte[14]	Durée du verrouillage du compte après le nombre de tentatives d'accès.	30Mn
Nombre de tentatives de connexions invalides	Nombre maximum de tentatives d'accès avant le verrouillage automatique du compte.	5
Réinitialiser le compteur de verrouillage de compte[15]	Délai avant le déverrouillage automatique du compte qui a été verrouillé automatiquement après un accès invalide.	1heure
Durée maximale du mot de passe (jours)	Durée maximale de la validité d'un nouveau mot de passe.	90 jours
Durée minimale du mot de passe	Durée minimale de la validité d'un nouveau mot de passe. C'est la durée qui doit s'écouler avant que l'utilisateur puisse changer de mot de passe.	1 jour
Longueur minimale du mot de passe (caractères)	Règle pour la création d'un mot de passe par l'utilisateur.	8 caractères
Longueur de l'historique du mot de passe	Nombre d'anciens mots de passe à ne pas réutiliser lors des changements de mots de passe.	10 derniers mots de passe
Complexité du mot de passe	Règle de création d'un mot de passe : utilisez des caractères majuscules, minuscules et des chiffres. Le mot de passe ne doit pas contenir le nom d'utilisateur du compte, ni le nom ou le prénom de l'utilisateur et peut contenir des caractères spéciaux.	Activé

[13] 64 mesures obligatoires du CGGAI – Volet sécurité, extrait de la CGGAI appartenant aux organismes du réseau de la santé et des services sociaux V2007-03-12 (représente toujours une référence de bonne pratique)
[14] Bonne pratique de stratégie de gestion de compte Windows : source Microsoft : https://technet.microsoft.com/fr-fr/library/hh994569(v=ws.11).aspx
[15] Bonne pratique de stratégie de gestion de compte Windows : source Microsoft : https://technet.microsoft.com/fr-fr/library/hh994568(v=ws.11).aspx

ANNEXE 2 : Périmètre de sécurité pour l'accès à l'information