Université de Montréal

Faculté de médecine
Vice-décanat des études médicales postdoctorales

Guide des études médicales postdoctorales pour les Comités de Compétence[1]

Chaque programme de résidence accrédité par le Collège royal des médecins et chirurgiens du Canada ou par le Collège des médecins de famille du Canada doit constituer un comité de compétence.

Le comité de compétence est responsable de faire une recommandation au comité de programme sur la préparation des résidents à progresser vers la prochaine étape de prise de responsabilité, telle que prévue au curriculum

Le comité de compétence :

- se réfère au "Guide d'évaluation du résident[1]" de la faculté de médecine de l'Université de Montréal
- utilise une diversité de données pour juger de la progression du résident
- revoit les tendances en termes de performance (entre les résidents, en fonction du stade de développement des compétences, selon les milieu d'apprentissage, les outils utilisés) afin d'identifier les points à améliorer pour les résidents individuellement et pour le programme globalement
- peut proposer un plan de soutien ou de remédiation pour le résident au comité de programme

Le cadre de référence et les recommandations issus du comité de compétence doivent être documentés et approuvés par le comité de programme (CP).

Le cadre de référence documente les éléments suivants :

Mandat

Structure

- Composition du comité
- Processus de nomination du responsable du comité
- Rôle du directeur de programme au sein du comité
- Participation et rôle du résident au sein du comité (note : il est recommandé qu'il y ait un résident au sein du comité, que ce dernier soit élu par les pairs et que le processus de sélection soit connu et accepté par les résidents du programme, ce résident pouvant être issu du programme ou d'un autre programme au besoin)
- Participation et rôle des autres membres au sein du comité s'il y a lieu (professeur ou directeur d'un autre programme, membre du public, patient, etc.)

[1] Ce guide s'applique aux programmes au moment de l'implantation officielle de la Compétence par Conception (CPC). Les autres programmes peuvent utiliser ce guide s'il est approuvé par le comité de programme

- Conflit d'intérêt des superviseurs envers les résidents (note : le document décrit l'obligation de la divulgation du conflit d'intérêt et l'abstention de vote ou même de participation ou d'assistance aux discussions le cas échéant. Mentionner que c'est au président du comité de compétence de juger si le conflit est significatif.)
- Description des accès aux données des résidents

Rôles et responsabilités

- Décrire les règles de confidentialité

Processus organisationnel

- Format (i.e. face-à-face ou à distance)
- Quorum pour les décisions
- Quand et comment les dossiers des résidents seront revus
- Comment les dossiers sont présentés
- Forme de votes acceptables (i.e. vote par courriel ou autres)
- Comment une égalité des votes est départagée (i.e. par le président du comité idéalement)
- Le rôle du comité de programme dans la ratification des décisions du comité et statuer si le(s) résident(s), membre(s) du comité de programme est(sont) présent(s) ou non pendant ce processus.

Processus décisionnel

- Comment les données sont collectées, circulées et entreposées pour s'assurer du respect de la confidentialité
- Les documents revus par le comité :
- I.e. Les données d'évaluation collectées pendant une période donnée et la revue des données antérieures pour apprécier la progression du résident.
- Mentionner qu'une expérience individuelle d'un membre du comité avec un résident ne peut être utilisée à moins qu'elle ne soit documentée
- Comment et par qui les décisions sont communiquées au comité de programme (idéalement par le président du comité de compétences)
- Comment et par qui les décisions sont communiquées au résident (idéalement par le directeur du programme)

Décisions possibles

- I.e. progression à la prochaine étape de développement des compétences, promotion d'une année de résidence à une autre, éligibilité à l'examen de certification, complétion de la formation, nécessité d'établir un plan de soutien ou de remédiation ou exclusion du programme.

Adoptée par le Comité des études médicales postdoctorales
(2019-CEMP-32-res01), 23 janvier 2019

ANNEXE A

Cadre de référence du comité de compétences du programme *inscrire le nom du programme*

Approuvé par le comité de programme le : inscrire la date

Mandat

Le comité de compétence effectue l'évaluation rigoureuse et transparente du rendement des résidents. Il a pour but de s'assurer que tous les apprenants satisfont aux exigences de la discipline en procédant à une synthèse et à un examen des données d'évaluation qualitatives et quantitatives à chaque étape de la formation, et de recommander de futures activités d'apprentissage.

Composition

Décrire ici la composition de votre comité, les éléments suivants vous guideront.

Le comité de compétence est présidé par quelqu'un d'autre que le directeur de programme. Le directeur de programme est invité à siéger au comité. La taille du comité doit refléter le nombre de résidents inscrits au programme; un minimum de trois membres est requis pour les petits programmes. Normalement, les membres du comité proviennent du comité du programme de résidence ou sont des superviseurs cliniques associés au programme. Il peut être utile d'inclure un membre qui ne fait pas partie du corps professoral. Cette personne peut être un professeur ou un directeur de programme provenant d'autres programmes de résidence offerts par l'université ou de la même discipline dans une autre université, ou encore un autre professionnel de la santé ou un membre public.

Rôles

Le comité de compétence évalue la progression des résidents en fonction des normes nationales de la discipline, et prend les décisions qui s'imposent.

Responsabilités et pouvoirs

Relevant du comité du programme de résidence, le comité de compétence doit :

- Suivre la progression de chaque résident en s'assurant que les activités professionnelles confiables (APC) ou les différents jalons de compétence ont été réalisés à chaque étape du programme.

- Avec l'aide des réviseurs principaux, faire une synthèse des résultats de différentes évaluations et observations (par le biais du document en annexe B ou à l'aide d'un autre outil permettant de structurer l'information présentée de façon consistante d'un dossier à l'autre) afin de prendre des décisions concernant:

    - le passage des résidents à la prochaine étape de la formation;
    - l'évaluation et l'approbation des plans d'apprentissage individuels élaborés pour cibler les points à améliorer;
    - l'état de préparation des résidents à se présenter aux examens du Collège royal;
    - l'état de préparation des résidents à exercer de façon autonome après avoir franchi l'étape de transition vers la pratique;
    - l'incapacité d'un stagiaire à progresser au sein du programme;
    - les résultats escomptés de tout plan de soutien ou de remédiation établi pour un résident en particulier.

- Assurer le maintien de la confidentialité et la promotion de la confiance par l'échange

d'information uniquement avec les personnes qui participent directement à l'élaboration ou à la mise en œuvre des plans d'apprentissage ou d'amélioration.

- S'engager à respecter la confidentialité des données sur les résidents par la signature, en début de mandat, d'un document conçu à cette fin (annexe C). Au début de chaque comité, le premier point à l'ordre du jour visera à faire un rappel de cet engagement de la part de chacun des membres.

- Respecter le processus établi dans le "Guide d'évaluation de l'Université de Montréal.

- Revoit les tendances en termes de performance (entre les résidents, en fonction du stade de développement des compétences, selon les milieux d'apprentissage, les outils utilisés) afin d'identifier les points à améliorer pour les résidents individuellement et pour le programme globalement.

Structure

- Le président du comité est proposé par le directeur de programme et nommé par le comité de programme pour un mandat d'une durée de deux ans, pouvant être renouvelé.
- Le directeur de programme siège sur le comité et participe aux discussions et aux votes (ou non).
- La participation des autres membres du comité est entérinée par le comité de programme.
- Un résident siège sur le comité, celui-ci est élu par ses pairs par le processus suivant : (décrire le processus qui convient à votre programme et qui est entériné par les résidents, le résident élu pouvant faire partie ou non du programme en question).
- Les membres doivent divulguer un conflit d'intérêt envers les résidents du programme (relation d'ordre familial ou autre). Le président du comité est responsable de juger s'il y a effectivement conflit d'intérêt justifiant une telle divulgation.
- Seuls les membres du comité de compétence peuvent avoir accès aux données d'évaluation des résidents
- Dès qu'un membre se retire du comité, il doit se voir retirer l'accès aux données des résidents, outre ceux qu'il évaluera à titre de professeur au quotidien.

Processus organisationnel

- Le comité peut se rencontrer en personne, en conférence téléphonique ou par zoom.
- Le quorum pour une décision est au minimum de trois membres (vous pouvez décider d'un nombre plus élevé mais pas plus bas, idéalement impair).
- Les votes ou ratifications par courriel sont acceptés (ou non, vous décidez).
- Le comité de programme doit entériner les décisions du comité de compétence (préciser si ce sera avec ou sans la présence du(des) résident(s), choisissez l'option qui convient le mieux à votre réalité et qui est acceptée par les résidents du programme).

Processus décisionnel

- Un réviseur principal présentera les données du résident selon le format requis.
- Les autres membres du comité de compétence auront accès aux données et pourront les consulter en ligne lors de la revue du dossier. Hormis le président du comité, le réviseur principal du dossier étudié et le directeur de programme, les autres membres n'accèderont pas à ces données en dehors des rencontres du comité.
- Les données résumées ne seront pas distribuées aux membres par courriel ni sous format papier avant, pendant ni après les rencontres.
- Les décisions sont basées sur l'information disponible au moment de la revue.

- Le comité considèrera les performances récentes du résident, sa progression dans le temps et la sécurité des patients.
- L'expérience individuelle d'un membre du comité ne peut être incluse si elle n'a pas été discutée avec le résident concerné et par la suite documentée au portfolio ou dans MedSIS.
- Les décisions seront habituellement prises par consensus, mais un vote formel sera effectué pour approuver les décisions et en cas d'égalité des votes, le président est celui qui tranchera la décision.
- La sélection des dossiers à présenter est faite en fonction des besoins : progression vers une étape ultérieure de développement, inquiétudes soulevées par rapport à la progression d'un résident ou la sécurité des patients ou si 6 mois de formation se sont écoulés depuis la dernière révision.
- Les politiques de l'Université quant à la confidentialité et la conservation des données s'appliquent.
- Le comité se réunit à la fréquence requise permettant d'assurer que chaque dossier de résident est revu au moins 2 fois par année et aussi souvent que nécessaire pour transiter sans délai vers une étape ultérieure de développement des compétences (établir un calendrier selon votre réalité).
- Le comité de compétence soumet un résumé écrit anonyme des décisions prises (voir annexe B).
- Le président du comité d'évaluation ou un délégué (réviseur principal, directeur de programme…) rencontre les résidents individuellement pour les informer des décisions prises et des recommandations émises.
- Les membres qui ont un conflit d'intérêt à l'égard d'un résident particulier doivent s'abstenir de voter sur les décisions le concernant. Il peut également être appelé à se retirer lors des discussions. Le président du comité est celui qui est responsable de juger des mesures appropriées pour minimiser les biais, le cas échéant.

Décisions possibles

- Progression attendue au sein de l'étape ou à une autre étape de développement.
- Promotion à la prochaine année de résidence.
- Confirmation de l'éligibilité à l'examen de certification.
- Confirmation de la complétion du programme de formation.
- Identification de résidents nécessitant des mesures de soutien pour leur progression.
- Identification de résidents ayant besoin de mesures de remédiation.
- Identification de préoccupations en lien avec la sécurité des patients ou des résidents.
- Identification de préoccupations en lien avec le bien-être des résidents.
- Identification de résidents éligibles à des activités ou programme d'enrichissement en raison d'une progression hors du commun.

ANNEXE B

RAPPORT DU COMITÉ DE COMPÉTENCE

Date de la révision en comité (JJ/MM/AAAA)

Nom et prénom du résident

Niveau actuel de l'apprenant (cocher)

Transition à la discipline	☐
Fondements	☐
Maitrise de la discipline	☐
Transition à la pratique	☐

Période révisée De : / Période À : / Période

Nombre total d'APCs observées

Éléments revus (cocher)

Eportfolio (APC et autres)	☐	Examen écrit local	☐
Fiches d'évaluation de stage	☐	Examen écrit national (AKT)	☐
Examen oral bi-annuel	☐	Rétroaction multi-sources	☐
Exercices d'observation directe	☐	Présentations orales	☐
Examen de simulation (CanNASC)	☐	Projet de recherche ou érudition	☐

Notes de révision
(incluant points forts et points à améliorer) :

Décision du comité de compétences (cocher)

Progresse tel qu'attendu ☐

- Suivre les progrès du résident ☐
- Modifier le plan d'apprentissage ☐
- Faire passer le résident à l'étape 2 ☐
- Faire passer le résident à l'étape 3 ☐
- Faire passer le résident à l'étape 4 – Admissible à l'examen du Collège royal ☐
- Faire passer le résident – Admissible à la certification du Collège royal ☐

Nécessite un plan de soutien (Ne progresse pas comme prévu) ☐

Nécessite un plan de remédiation (problématique majeure ou récurrente ou n'arrive pas à progresser) ☐

Retrait de la formation ☐

Progresse au-delà des attentes* ☐

- Modifier le plan d'apprentissage (parfaire des compétences particulières) ☐
- Faire passer le résident – Admissible à l'examen du Collège royal ☐

Faire passer le résident à l'étape 4	
Faire passer le résident – Admissible à la certification du Collège royal	

*Seulement possible si à la fin de l'étape de la maitrise de la discipline ou à celle de transition à la pratique

Recommandations pour le développement

Signature du président du comité de compétence

En général, cette évaluation reflète mes performances	oui		non	
J'ai rencontré mes superviseurs et j'ai discuté de mon évaluation	oui		non	

Signature du résident

ANNEXE B

ENGAGEMENT DE CONFIDENTIALITÉ APPLICABLE AUX RENSEIGNEMENTS PERSONNELS AUXQUELS LE SIGNATAIRE A ACCÈS DANS L'EXERCICE DE SES FONCTIONS À L'UNIVERSITÉ DE MONTRÉAL[2]

Attendu que l'Université de Montréal est tenue, en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, d'assurer la confidentialité des renseignements personnels qu'elle recueille et détient ;

Attendu que dans le cadre de mes fonctions je peux avoir à accès à de tels renseignements.

Je, soussignée, (prénom et nom) _____

Matricule _____

M'engage à respecter la confidentialité des renseignements personnels auxquels j'aurai accès dans l'exercice de mes fonctions.

Je reconnais avoir pris connaissance de la Politique de sécurité de l'information 40.28 ainsi que la Directive relative à l'utilisation du courrier électronique 40.20, et m'engage à les respecter.

Plus particulièrement, je m'engage :

1. à n'accéder qu'aux renseignements nécessaires à l'exécution de mes tâches;
2. à n'utiliser ces renseignements que dans le cadre de mes fonctions;
3. à ne révéler aucun renseignement personnel dont j'aurai pris connaissance dans l'exercice de mes fonctions à moins d'y être dûment autorisé;
4. à n'intégrer ces renseignements que dans les seuls dossiers prévus pour l'accomplissement des mandats qui me sont confiés;
5. à conserver ces dossiers de sorte que seules les personnes autorisées puissent y avoir accès;
6. à protéger par un mot de passe, l'accès à l'information confidentielle que je détiens ou à laquelle j'ai accès;
7. à disposer, s'ils contiennent des renseignements personnels, de tout papier rebut par déchiquetage;
8. à informer sans délai mes supérieurs de toute situation ou irrégularité qui pourrait compromettre de quelque façon la sécurité, l'intégrité ou la confidentialité des renseignements détenus par mon employeur;
9. à ne conserver à la fin de l'emploi ou du contrat aucun renseignement personnel transmis ou recueilli dans le cadre de mes fonctions et à maintenir mon obligation de confidentialité à leur égard.

En foi de quoi, j'ai signé à _____ , ce _____

Nom Titre

Signature _____

[2] L'exemplaire principal de ce document doit être conservé dans le dossier de l'employé conservé à la Direction des ressources humaines. Un exemplaire secondaire peut être conservé dans le dossier de l'employé de l'unité concernée.

ANNEXE C

Université de Montréal

RECUEIL OFFICIEL
RÈGLEMENTS, DIRECTIVES, POLITIQUES ET PROCÉDURES

Secrétariat général

GESTION COURANTE	Numéro : 40.28		Page 1 de 13
POLITIQUE DE SÉCURITÉ DE L'INFORMATION	Adoption Date : 2005-01-11	Délibération : E-965-12	
	Modifications Date : 2015-09-28	Délibération : CU-0624-5.4	Article(s) :

TABLE DES MATIÈRES

GESTION COURANTE	Numéro : 40.28		Page 2 de 13
POLITIQUE DE SÉCURITÉ DE L'INFORMATION	Adoption Date : 2005-01-11	Délibération : E-965-12	
	Modifications Date : 2015-09-28	Délibération : CU-0624-5.4	Article(s) :

1. PRÉAMBULE[1]

Dans l'accomplissement de sa mission, l'Université de Montréal détient de l'Information sous plusieurs formes et sur plusieurs supports. Cette Information doit faire l'objet d'une utilisation appropriée et d'une protection adéquate tout au long de son Cycle de vie. La présente Politique est adoptée afin d'encadrer la Sécurité de l'information et la protection des Actifs informationnels de l'Université, en complémentarité avec la Politique de gestion de l'information (10.47).

2. OBJECTIFS

La présente Politique a pour objectif d'assurer la Sécurité de l'information tout au long de son Cycle de vie, et plus précisément :

- la Disponibilité de l'Information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise aux personnes autorisées;
- l'Intégrité de l'Information de manière à ce que celle-ci ne soit pas détruite ni altérée de quelque façon sans autorisation, et que le support de cette Information lui procure la stabilité et la pérennité voulues;
- la Confidentialité de l'Information, en limitant la divulgation et l'utilisation de celle-ci aux seules personnes autorisées;
- le soutien à l'encadrement et à la mise en œuvre du cadre normatif interne en matière de Sécurité de l'information;
- le maintien de systèmes et de contrôles internes offrant une assurance raisonnable de conformité à l'égard des lois, directives et pratiques gouvernementales en la matière.

3. CADRE LÉGAL ET NORMATIF

La Politique de Sécurité de l'information s'inscrit notamment dans un contexte régi par :

- la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (L.R.Q., c. G-1.03);
- la *Loi concernant le cadre juridique des technologies et l'information* (L.R.Q., c. C-1.1);

[1] Les termes commençant par une lettre majuscule employés dans la présente Politique ont le sens qui leur est attribué dans le glossaire.

- la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1);
- la *Loi sur les archives* (L.R.Q. c. A-21.1);
- la *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics* (Décret no 261-2012 du 28 mars 2012);
- la *Directive sur la sécurité de l'information gouvernementale* (Décret 7-2014 du 15 janvier 2014);
- le *Cadre gouvernemental de gestion de la sécurité de l'information* (juin 2014).

De plus, l'Université a adopté au fil du temps les politiques suivantes :

- Politique de gestion de l'information (10.47);
- Politique sur la gestion de documents et les archives (10.49);
- Politique sur la protection des renseignements personnels (40.29);
- Politique sur la gestion des risques (10.45).

4. CHAMP D'APPLICATION

Le champ d'application de la présente Politique est le suivant :

4.1 Information et Actifs informationnels

L'Information et les Actifs informationnels visés sont ceux :

- appartenant à l'Université et détenus par elle;
- appartenant à l'Université, mais détenus par un consultant, un fournisseur, un partenaire, un organisme ou une firme externe;
- utilisés par un consultant, un fournisseur, un partenaire, un organisme ou une firme externe et détenus par lui au bénéfice ou pour et au nom de l'Université;

quel qu'en soit le support, incluant le papier.

4.2 Utilisateurs

Les Utilisateurs visés sont :

- les personnes à l'emploi de l'Université;
- les étudiants de l'Université;
- tout consultant, fournisseur, partenaire, invité, organisme ou firme externe autorisés à accéder, à exploiter ou à héberger l'Information et les Actifs informationnels de l'Université.

4.3 Activités

Les activités visées sont notamment celles visant la cueillette, la consultation, la production, la transmission, la conservation et la destruction de l'Information et des Actifs informationnels, peu importe leur support, leur emplacement, le moyen de communication, que ces activités soient conduites sur le campus de l'Université ou dans un autre lieu.

5. PRINCIPES DIRECTEURS

5.1 Rôles et responsabilités

L'efficacité des mesures de Sécurité de l'information exige l'attribution claire de rôles et de responsabilités aux différents intervenants de l'organisation dans la mise en place d'un cadre de gestion interne de la sécurité permettant une reddition de comptes adéquate.

5.2 Évolution

Les pratiques et les solutions retenues en matière de Sécurité de l'information doivent être réévaluées périodiquement afin de tenir compte des changements juridiques, organisationnels, technologiques, physiques et environnementaux, ainsi que de l'évolution des menaces et des risques.

5.3 Universalité

Les pratiques et les solutions retenues en matière de Sécurité de l'information doivent correspondre, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées à l'échelle nationale et internationale.

5.4 Éthique

Le cadre de gestion de la Sécurité de l'information repose sur des considérations éthiques visant à assurer la régulation des conduites et la responsabilisation individuelle.

6. CADRE DE GESTION

6.1 Gestion de la Sécurité de l'information

La Politique de Sécurité de l'information de l'Université s'articule autour des trois axes fondamentaux de gestion, soit la gestion des risques, la gestion de l'accès et la gestion des incidents.

6.1.1. Gestion des risques

Le niveau de protection de l'Information est établi en fonction :

- de son importance;
- des probabilités d'occurrence d'accident, d'erreur et de malveillance auxquels elle est exposée;
- des conséquences de la matérialisation de ces risques.

Une catégorisation à jour de l'Information assujettie à la présente Politique soutient l'analyse de risques ainsi que la détermination de sa valeur pour l'organisation.

L'analyse de risques guide également l'acquisition et le développement des Actifs informationnels, en spécifiant les mesures de sécurité à mettre en œuvre pour leur déploiement dans l'environnement de l'Université. La gestion des risques reliés à la Sécurité de l'information s'inscrit dans le processus global de gestion des risques de l'Université.

6.1.2. Gestion de l'accès

La Sécurité de l'information est assurée par des mesures d'encadrement et un contrôle adéquat sur l'accès, la divulgation et l'utilisation de l'Information par les personnes autorisées, afin d'en protéger la Confidentialité et l'Intégrité, en portant une attention particulière à l'information confidentielle et aux renseignements personnels.

L'efficacité des mesures de Sécurité de l'information repose sur l'attribution de responsabilités et une imputabilité des Utilisateurs, à tous les niveaux de l'organisation.

6.1.3. Gestion des incidents

L'Université déploie des mesures de Sécurité de l'information afin d'assurer la continuité de ses services. À cet égard, elle met en place les mesures nécessaires afin de :

- limiter l'occurrence des Incidents en matière de Sécurité de l'information;
- gérer adéquatement ces Incidents pour en minimiser les conséquences et rétablir la situation.

Dans la gestion des Incidents, l'Université peut exercer ses pouvoirs et ses prérogatives eu égard à toute utilisation inappropriée de l'Information et d'Actifs informationnels qu'elle détient, notamment en matière de relations de travail et d'enquêtes criminelles, en vertu des dispositions applicables en la matière.

6.2 Rôles et responsabilités

Les rôles et les responsabilités des différents intervenants en matière de Sécurité de l'information sont les suivants :

6.2.1. Conseil

- Le Conseil adopte la Politique de Sécurité de l'Information ainsi que toute modification à celle-ci.

6.2.2. Secrétaire général

Le Secrétaire général assume le rôle de Responsable organisationnel de la Sécurité de l'information (ROSI) au sein de l'Université. À cet égard, il :

- représente l'Université en matière de Sécurité de l'information;
- est responsable de l'application de la présente Politique;
- fait adopter les orientations stratégiques, les plans d'action et le cadre normatif en matière de Sécurité de l'information;
- s'assure de la mise en œuvre et de l'adéquation des mesures permettant de réduire les Risques de Sécurité de l'information à un niveau acceptable pour l'Université;

- s'assure que les ententes de services et les contrats conclus avec des fournisseurs, des partenaires, des consultants et des organismes externes sont conformes aux exigences en matière de Sécurité de l'information;
- approuve et transmet aux instances gouvernementales concernées les documents afférents à la reddition de comptes, notamment les plans d'action et les bilans requis, conformément à la *Directive sur la sécurité de l'information gouvernementale*;
- s'assure de la déclaration, par l'Université, des Risques et des Incidents de Sécurité de l'information à portée gouvernementale;
- s'assure que le Registre d'autorité de la Sécurité de l'information est tenu à jour.

6.2.3. Comité de direction

Le Comité de direction adopte les orientations stratégiques, les plans d'action et le cadre normatif en matière de Sécurité de l'information.

6.2.4. Comité sur la gestion de l'information

Constitué en vertu de la *Politique de gestion de l'information*, le Comité sur la gestion de l'information est la principale instance de concertation en matière de Sécurité de l'information, au niveau stratégique, au sein de l'Université.

6.2.5. Direction générale des technologies de l'information et la communication (DGTIC)

La DGTIC :

- recommande au ROSI pour approbation, en matière de Sécurité de l'information, les orientations stratégiques, les plans d'action, et le cadre normatif et en assure ensuite la mise en œuvre;
- s'assure de la prise en charge des exigences de Sécurité de l'information dans l'exploitation des systèmes d'information, ainsi que lors de la réalisation de projets de développement et de l'acquisition de systèmes d'information;
- communique au sein de l'organisation les orientations et les priorités d'intervention gouvernementales en matière de Sécurité de l'information;

- sensibilise les membres de la Communauté universitaire :
  - à la Sécurité de l'information et des Actifs informationnels;
  - aux conséquences d'une atteinte à leur sécurité;
  - à leur rôle et à leurs obligations en la matière.
- assure la coordination et la cohérence des actions menées au sein de l'Université en matière de Sécurité de l'information, notamment par les Détenteurs de l'Information ainsi que par les Unités en matière de :
  - gestion des risques;
  - gestion de l'accès;
  - gestion des incidents;
  - sécurité physique.
- s'assure de la réalisation périodique d'audits de Sécurité de l'information et de tests d'intrusion et de vulnérabilités, et en dégage les priorités;
- assure la continuité des services et la mise en œuvre du plan de relève, lorsque requis; assure la mise à jour des plans de relève et effectue les tests périodiques;
- tient à jour le Registre d'autorité de la Sécurité de l'information;
- rend compte au Secrétaire général de ses réalisations en matière de Sécurité de l'information;
- s'assure de la participation de l'Université aux comités relatifs à la Sécurité de l'information.

6.2.6. Officier de sécurité informatique

L'officier de sécurité informatique assume les rôles de Conseiller organisationnel en sécurité de l'information (COSI) et de Coordonnateur organisationnel de gestion des incidents (COGI); il soutient le ROSI en contribuant notamment à la mise en œuvre des mesures d'atténuation des Risques et à la mise en place des processus de Sécurité de l'information. À cet égard, il :

- conçoit et met en œuvre l'architecture de Sécurité de l'information et arrime les solutions retenues aux processus organisationnels de Sécurité de l'information;

- assiste les Détenteurs de l'Information en matière de catégorisation et d'analyse des Risques de Sécurité de l'information sous leur responsabilité;
- coordonne la mise en œuvre des processus de Sécurité de l'information;
- contribue à l'analyse des Risques de Sécurité de l'information, identifie les menaces et les situations de vulnérabilité, et met en œuvre les solutions appropriées;
- coordonne la gestion des Incidents et met en œuvre les stratégies de réaction appropriées;
- tient à jour le registre des Incidents, documente ces Incidents et en tient informés le ROSI, la DGTIC et le Comité sur la gestion de l'information pour les Incidents critiques;
- produit les plans d'action et les bilans de l'Université en matière de Sécurité de l'information;
- contribue au processus d'acquisition de biens et de services afin de s'assurer que les ententes de services et les contrats intègrent des dispositions afin de respecter les exigences en matière de Sécurité de l'information;
- collabore à l'élaboration du contenu du programme de sensibilisation et d'information en matière de Sécurité de l'information;
- fournit un soutien dans le cadre des enquêtes de sécurité informatique.

6.2.7. Gestionnaires d'unités académiques et administratives, et responsables informatiques

Les gestionnaires d'Unités académiques et administratives, et les responsables informatiques :

- informent le personnel relevant de leur autorité de la Politique de Sécurité de l'information et des dispositions du cadre normatif, afin de le sensibiliser à la nécessité de s'y conformer;
- protègent l'Information et les Actifs informationnels sous leur responsabilité dans leur Unité, en s'assurant que ceux-ci sont utilisés par le personnel relevant de leur autorité en conformité avec les principes directeurs et les exigences de la Politique de Sécurité de l'information et du cadre normatif;
- s'assurent que les exigences en matière de Sécurité de l'information sont prises en compte dans tout processus d'acquisition et contrat de service sous leur responsabilité, et voient à ce que tout consultant, fournisseur, partenaire, invité, organisme ou firme externe s'engagent à respecter et respectent la Politique et le cadre normatif en découlant;
- rapportent au Secrétaire général tout problème lié à l'application de la présente Politique;

- rapportent à la DGTIC tout incident afférant à la Sécurité de l'information.

6.2.8. Utilisateurs

La responsabilité de la Sécurité de l'information de l'Université incombe à tous les Utilisateurs.

Tout Utilisateur qui accède à de l'Information, la consulte ou la traite est responsable de l'utilisation qu'il en fait et doit procéder de manière à protéger cette Information.

À cette fin, il doit :

- se conformer à la présente Politique et au cadre normatif en découlant;
- utiliser les droits d'accès qui lui sont attribués, l'Information et les Actifs informationnels mis à sa disposition uniquement dans le cadre de ses fonctions et aux fins auxquelles ils sont destinés;
- respecter les mesures de sécurité mises en place, ne pas les contourner ni modifier leur configuration ou les désactiver;
- signaler à la DGTIC tout Incident susceptible de constituer une contravention à la présente Politique ou de constituer une menace à la Sécurité de l'information de l'Université.

6.2.9. Direction de la prévention et de la sécurité (DPS)

La DPS met en place les mesures de protection physique des locaux et de sécurisation de leurs accès, notamment lorsqu'ils abritent des systèmes et des installations technologiques stratégiques ou essentielles ou des supports de l'Information confidentielle.

6.2.10. Direction des ressources humaines (DRH)

La DRH :

- informe et obtient de tout nouvel employé de l'Université son engagement au respect de la présente Politique et du cadre normatif en découlant;
- met en place les programmes de sensibilisation et d'information des employés de l'Université en matière de Sécurité de l'information.

6.2.11. Bureau de la vérification interne (BVI)

Le BVI évalue, examine ou vérifie notamment :

- l'application, la validité et l'efficacité des plans d'action, du cadre normatif et des moyens technologiques élaborés et mis en œuvre en matière de Sécurité de l'information;
- le respect du cadre de gestion afférent à la Sécurité de l'information et des Actifs informationnels.

7. SENSIBILISATION ET INFORMATION

La Sécurité de l'information repose notamment sur la régulation des conduites et la responsabilisation individuelle. À cet égard, les membres de la Communauté universitaire doivent être sensibilisés :

- à la Sécurité de l'information et des Actifs informationnels;
- aux conséquences d'une atteinte à la Sécurité;
- à leur rôle et à leurs responsabilités en la matière.

8. SANCTIONS

Tout membre de la Communauté universitaire qui contrevient au cadre légal, à la présente Politique et aux mesures de Sécurité de l'information qui en découlent s'expose à des sanctions selon la nature, la gravité et les conséquences de la contravention, en vertu de la loi, du règlement disciplinaire applicable et du droit du travail.

De plus, en cas de contravention, l'Utilisateur engage sa responsabilité personnelle; il en est de même pour l'Utilisateur qui, par négligence ou par omission, a fait en sorte que l'Information ne soit pas protégée adéquatement.

De même, toute contravention par un fournisseur, un partenaire, un invité, un consultant ou un organisme externe l'expose aux sanctions prévues au contrat le liant à l'Université ou en vertu des dispositions de la législation applicable en la matière.

9. GLOSSAIRE

Actif informationnel : Une information, quel que soit son canal de communication (téléphone, réseau de télécommunication, voix, etc.) ou son support (papier, pellicule photographique ou cinématographique, ruban magnétique, support électronique, disque dur, etc.), un système ou une technologie de l'information ou un ensemble de ces éléments.

Cadre normatif : Ensemble de normes, notamment une politique, un règlement, une directive, un standard, un processus qui encadrent les activités d'une organisation.

Communauté universitaire : Ensemble des employés et des étudiants de l'Université, excluant les écoles affiliées.

Confidentialité : Propriété d'une information qui n'est accessible qu'aux personnes ou entités désignées et autorisées et qui n'est divulguée qu'à celles-ci.

Cycle de vie de l'information : Ensemble des étapes que franchit une information et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation de l'Université.

Détenteur de l'information : Toute personne qui, dans le cadre de ses fonctions, conserve l'information que l'Université détient dans l'accomplissement de sa mission, ainsi que les ressources qui la sous-tendent.

Disponibilité : Propriété d'une information d'être accessible en temps voulu et de la manière requise à une personne autorisée.

Incident : Événement qui porte atteinte ou qui est susceptible de porter atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information, ou plus généralement à la sécurité des actifs informationnels, notamment une interruption des services ou une réduction de leur qualité.

Information : Renseignements consignés sur un support quelconque pour être conservés, traités ou communiqués comme éléments de connaissance.

Intégrité : Propriété d'une information qui ne subit aucune altération ni destruction sans autorisation ou de façon erronée, et qui est conservée sur un support lui procurant stabilité et pérennité. L'intégrité fait référence à l'exactitude et à la complétude.

Registre d'autorité : Registre dans lequel sont notamment consignés les noms des détenteurs de l'information ainsi que les systèmes d'information qui leur sont assignés.

GESTION COURANTE	Numéro : 40.28		Page 13 de 13
POLITIQUE DE SÉCURITÉ DE L'INFORMATION	Adoption Date : 2005-01-11	Délibération : E-965-12	
	Modifications Date : 2015-09-28	Délibération : CU-0624-5.4	Article(s) :

Risque de sécurité de l'information : Risque d'interruption ou de réduction de la qualité des services, ou d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information et qui peut avoir des conséquences sur la prestation des services, sur la vie, la santé ou le bien-être des personnes, sur le respect de leurs droits fondamentaux à la protection des renseignements personnels et au respect de leur vie privée, ainsi que sur l'image de l'Université.

Sécurité de l'information : Protection de l'information et des actifs informationnels contre les risques et les incidents.

Unité : L'un ou l'autre des facultés, écoles, départements, services administratifs, ainsi que l'une ou l'autre des unités de recherche constituées par le Comité exécutif de l'Université.

ANNEXE E

Université de Montréal

Secrétariat général

RECUEIL OFFICIEL
RÈGLEMENTS, DIRECTIVES,
POLITIQUES ET PROCÉDURES

GESTION COURANTE	Numéro : 40.20		Page 1 de 2
DIRECTIVE RELATIVE À L'UTILISATION DU COURRIER ÉLECTRONIQUE	Adoption Date : 1999-03-15	Délibération :	
	Modifications Date :	Délibération :	Article(s) :

Encore inusité il y a quelques années, le courrier électronique (courriel) est maintenant devenu un outil de travail usuel. Ses avantages sont indéniables : convivialité, rapidité et efficacité. La présente directive vise à vous renseigner sur divers aspects du courriel et à vous indiquer les précautions à prendre lorsque vous utilisez ce médium comme moyen de communication dans le cadre de vos fonctions à l'Université de Montréal.

1- LE COURRIEL N'EST PAS UN SUBSTITUT À UNE CONVERSATION TÉLÉPHONIQUE

Contrairement à une croyance largement répandue, le courriel n'est pas un substitut à une conversation téléphonique. Les renseignements que l'on communique par ce médium sont fixés sur un support. Dès lors, le courriel constitue un document et doit être traité comme tel.

2- LE COURRIEL EST UN DOCUMENT SOUMIS À L'ACCÈS À L'INFORMATION ET AUX RÈGLES DE CONSERVATION DES ARCHIVES DE L'UNIVERSITÉ

Le courriel doit être traité au plan de l'accès à l'information et au plan archivistique comme n'importe quel autre document détenu par l'Université. La loi ne fait pas de distinction entre la forme que peuvent prendre les documents, qu'elle soit écrite, graphique, sonore, visuelle, informatisée ou autre.

Les règles d'accès et d'exclusion à l'accès prévues par la loi, de même que celles relatives à la protection des renseignements personnels, s'appliquent au courriel détenu par l'Université comme à n'importe quel autre document.

Concernant la détention du document, sachez que même si vous supprimez un courriel à partir de votre poste de travail, une copie pourrait exister et demeurer intact pendant un certain temps dans les copies de sécurité des serveurs de courrier électronique de l'Université.

Les règles de conservation des documents produits sur courriel sont les mêmes que celles visant l'ensemble des documents : ces règles s'appliquent en fonction du contenu du document et non en fonction de son support. Il faut se référer au Calendrier général des règles de conservation des documents de l'Université, qui a été adopté par la Commission des archives de l'Université et que l'on peut consulter en s'adressant à la Division des archives du Secrétariat général.

Au sein du sous-comité des archivistes de la CREPUQ, des mesures sont actuellement considérées pour assurer la gestion adéquate des documents électroniques, tels les courriels. Divers modèles – dont certains prévoient un recours à l'intranet – sont en voie d'être expérimentés. Ces bancs d'essai, menés parallèlement avec des projets similaires réalisés au niveau gouvernemental, devraient permettre de préciser une éventuelle politique de conservation des documents électroniques et, par conséquent, de recommander un support d'information à privilégier à moyen et à long termes en ce domaine.

D'ici là, les usagers du courriel sont invités à conserver sur support papier les documents à valeur légale ou historique, ainsi que ceux témoignant des activités importantes de leur secteur.

3- LE COURRIEL N'OFFRE AUCUNE GARANTIE DE CONFIDENTIALITÉ

Il n'y a aucune garantie de confidentialité des documents produits sur courriel. Les risques d'indiscrétion sont proportionnels au nombre de sites sur lesquels le courriel transite pour se rendre à destination.