GESTION COURANTE Numéro **:** 40.28 Page 1 de 14

POLITIQUE DE SÉCURITÉ DE L'INFORMATION

Adoption
Date : 2005-01-11
Délibération : E-965-12

Modifications

Date :	Délibération :	Article(s) :
2015-09-28	CU-0624-5.4	
2020-11-03	Secrétariat général	6.2.11
2024-02-13	E-0186-5.1	

TABLE DES MATIÈRES

Adoption		
Date :	Délibération :	
2005-01-11	E-965-12	
Modifications		
Date :	Délibération :	Article(s) :
2015-09-28	CU-0624-5.4	
2020-11-03	Secrétariat général	6.2.11
2024-02-13	E-0186-5.1	

Adoption
Date : 2005-01-11
Délibération : E-965-12

Modifications

Date :	Délibération :	Article(s) :
2015-09-28	CU-0624-5.4	
2020-11-03	Secrétariat général	6.2.11
2024-02-13	E-0186-5.1	

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'encadrer 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.

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

Adoption		
Date :	Délibération :	
2005-01-11	E-965-12	
Modifications		
Date :	Délibération :	Article(s) :
2015-09-28	CU-0624-5.4	
2020-11-03	Secrétariat général	6.2.11
2024-02-13	E-0186-5.1	

3. DÉFINITIONS

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, une installation ou un ensemble de ces éléments, acquis ou constitués par l'Université.

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.

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 santé financière de l'Université, sur la vie, la santé ou le bien-être des personnes, sur la santé et le bien-être des animaux dans les animaleries ou dans les cliniques de l'Université, sur le respect de leurs droits fondamentaux à la protection des renseignements personnels et au respect de leur vie privée, ainsi que sur la réputation de l'Université.

Sécurité de l'information : Ensemble de mesures mises en place pour assurer la protection des informations selon le niveau de confidentialité, d'intégrité et de disponibilité jugé nécessaire.

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.

4. CHAMP D'APPLICATION

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

4.1 Actifs informationnels

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;

et ce, 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, l'utilisation, 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 Identification des rôles et responsabilités des intervenants

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 Évaluation périodique des pratiques et solutions

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 Principe d'universalité et approche globale

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. Ces pratiques doivent être basées sur une approche globale qui tient compte des aspects financiers, organisationnels, humains, juridiques et technologiques.

5.4 Utilisation éthique des Actifs informationnels

Le cadre de gestion de la Sécurité de l'information repose sur des considérations éthiques visant à assurer la régulation des conduites, la responsabilisation individuelle et la pérennité d'une information fiable. Une démarche éthique permet notamment la responsabilisation collective et individuelle en plus de soutenir le processus de gestion de la sécurité de l'information.

5.5 Intégration de la Sécurité de l'information en amont

L'identification des besoins en sécurité de l'information dès le début des projets permet de protéger adéquatement les actifs informationnels en mettant en œuvre des mesures de sécurité appropriées dès leur conception ou leur acquisition. Ces mesures assurent autant la protection de l'information, tout au long de son cycle de vie, que la résilience des systèmes de l'université et des infrastructures critiques.

5.6 Catégorisation des Actifs informationnels

La catégorisation des Actifs informationnels est un élément essentiel de la Sécurité de l'information permettant d'appliquer les contrôles de sécurité adéquate. Les Actifs informationnels doivent être protégés selon le besoin en matière de disponibilité, d'intégrité et de confidentialité de façon à considérer les mesures applicables en sécurité de l'information. Le choix des mesures de protection s'appuie sur une analyse des risques auxquels l'information peut être exposée.

5.7 Identification et 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.

5.8 Processus formel de gestion des identités et des 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.

5.9 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.

5.10 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.

6. RÔLES ET RESPONSABILITÉS

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

6.1 Conseil

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

6.2 Comité sur les technologies de l'information, la protection des renseignements personnels, l'accès et la sécurité de l'information (CTIPRPASI)

Le CTIPRPASI donne des avis et fait des recommandations au Conseil sur les actions et décisions qu'il doit prendre en regard de la sécurité des systèmes d'information :

- pour établir le niveau de risque acceptable et approuver les orientations en matière de gestion de la sécurité de l'information

- pour recommander le financement requis pour la mise en œuvre de la stratégie en sécurité de l'information

- pour faire le suivi de l'avancement du plan d'action institutionnel et des plans d'action sectoriels en sécurité de l'information; et de la posture de sécurité, et de la saine gestion des risques associés.

Le CTIPRPASI répond également au Conseil de la gouvernance institutionnelle des technologies de l'information et de la communication (TIC), incluant la valorisation et la contribution des actifs informationnels de l'Institution.

6.3 Comité stratégique de la sécurité de l'information (CSSI)

Le CSSI relève du Conseil, est sous la responsabilité du CTIPRPASI et est présidé par le secrétaire général qui en est membre d'office. Le CSSI a comme objectifs et mandat :

- d'établir le niveau de risque acceptable et les orientations en matière de gestion de la sécurité de l'information;

- de recommander le financement requis pour la mise en œuvre de la stratégie en sécurité de l'information;

- d'effectuer les recommandations en matière de sécurité de l'information au Conseil;

- de diffuser les décisions en matière de sécurité de l'information au reste de l'institution;

- d'être responsable du respect des règles et de l'évolution de la gestion de la sécurité de l'information;

- d'effectuer le suivi de l'avancement du plan d'action institutionnel et des plans d'action sectoriels en sécurité de l'information; et de la posture de sécurité, et de la saine gestion des risques;

- d'approuver les directives de Sécurité de l'information;

- de gérer les exceptions aux politiques, aux lois et régulations provinciales/fédérales.

6.4 Chef de la sécurité de l'information organisationnelle (CSIO)

Le CSIO assume la responsabilité de la prise en charge globale de la sécurité de l'information au sein de l'université. Il travaille en étroite collaboration avec les répondants en matière de sécurité de l'information pour assurer la prise en charge des exigences de sécurité de. Il est notamment responsable :

- mettre en œuvre les décisions émanant du chef gouvernemental de la sécurité de l'information (CGSI) et du chef délégué de la sécurité de l'information (CDSI) auquel il se rattache, notamment les indications d'application et les indications d'application particulières, en coordonner l'exécution et veiller à leur application;

- contribuer à la mise en œuvre du cadre de gouvernance qui régit la sécurité de l'information au sein de l'université;

- contribuer à la mise en œuvre des processus gouvernementaux normalisés en matière de gestion de la sécurité de l'information et des processus de sécurité de l'information élaborés par le chef délégué de la sécurité de l'information (CDSI);

- s'assurer de la prise en charge des exigences de sécurité de l'information lors de la réalisation de projets de développement, d'acquisition, d'évolution ou de remplacement d'un actif informationnel ou d'un service en ressources informationnelles;

- aviser sans délai le chef délégué de la sécurité de l'information (CDSI) lorsqu'un événement de sécurité présente un risque qu'un préjudice sérieux soit causé;

- mettre en œuvre les actions requises pour la prise en charge d'un événement de sécurité;

- tenir un registre des événements de sécurité selon les exigences de la Directive et les modalités précisées par le chef délégué de la sécurité de l'information (CDSI);

- fournir les informations demandées par le chef gouvernemental de la sécurité de l'information (CGSI) et le chef délégué de la sécurité de l'information (CDSI) auquel il se rattache relativement à la reddition de comptes, ou toute autre information requise par ces derniers;

- mettre en place au sein de l'université les comités et les groupes de travail appropriés de concertation en matière de sécurité de l'information et en assurer la coordination;

- assurer le développement des compétences du personnel de l'université en matière de sécurité de l'information.

6.5 Coordonnateur organisationnel de mesures de sécurité de l'information (COMSI)

Le COMSI soutient le CSIO 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 :

- représente l'université auprès du Réseau d'alerte gouvernemental;

- produit les plans d'action et les bilans de l'Université en matière de Sécurité de l'information;

- il est responsable de l'application du processus de gestion des menaces, vulnérabilités et incidents (MVI) à l'université;

- Il est responsable de la prise en charge d'événements associés à des MVI;

- Identifie les MVI touchant l'université, en tenir informé son CSIO et les faire remonter selon les conditions définies par le processus GMVI;

- s'assure de l'élaboration, de la mise à jour et de l'application d'un plan interne de

- réponse aux MVI;

- 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;

- Collaborer étroitement avec son CSIO et son responsable opérationnel de cyberdéfense (ROCD) en leur fournissant, notamment, le soutien technique nécessaire à l'exercice de leurs responsabilités.

6.6 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 tout incident afférant à la Sécurité de l'information ou à la protection des renseignements personnels selon le processus en place.

6.7 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 ne modifier leur configuration ou les désactiver;

- Signaler selon les processus en vigueur toute situation portée à leur connaissance et qui est susceptible de constituer une atteinte potentielle à la sécurité de l'information et des renseignements personnels détenus par l'université;

- signaler 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.

7. SANCTIONS

Tout membre de la Communauté universitaire qui contrevient au cadre légal, à la présente Politique ou 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 qu'un Actif informationnel ne soit pas protégé adéquatement.

De même, toute contravention à la présente Politique et aux mesures de Sécurité de l'information 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 législatives applicables.

8. ENTRÉE EN VIGUEUR

La présente Politique entre en vigueur lors de son adoption par le Conseil de l'Université.