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

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.

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.