Politique sur la sécurité et la gestion des ressources informationnelles

Instance : Comité exécutif

	Date	Résolution
Adoption	14 décembre 2016	2016-9-CEX-R-37
Modifications	29 mai 2019	2019-5-CEX-R-27

Révisée le	29 mai 2019
Prochaine révision	29 mai 2022
Responsable	Vice-présidence à l'administration

Université du Québec

Table des matières

Préambule

L'Université du Québec doit prendre les meilleurs moyens à sa disposition pour protéger l'information qu'elle détient dans l'exercice de ses fonctions, que cette information soit sous forme numérique ou manuscrite. Le maintien des moyens et des mesures de sécurité des ressources informationnelles de l'Université est fondamental pour accomplir sa mission dans le respect des valeurs nécessaires au développement du savoir.

1 Énoncé de principe

La sécurité des ressources informationnelles vise notamment à maintenir des moyens adéquats pour assurer leur utilisation dans le cadre des activités de l'Université dans le respect des exigences de confidentialité, d'intégrité et de disponibilité.

Cette responsabilité repose sur les principes suivants :

- le respect des lois, règlements et politiques par les utilisateurs;
- la fiabilité, la qualité, la mise en œuvre de moyens afin de protéger le bon fonctionnement des ressources informationnelles;
- la recherche et la mise en œuvre d'outils pour l'utilisation optimale des ressources informationnelles pour des fins institutionnelles;
- une sensibilisation des utilisateurs à des comportements sécuritaires et responsables;
- l'information des utilisateurs sur les environnements informatiques, dont l'infonuagique impliquant notamment la garde de banques de données sur des serveurs externes;
- le respect des droits des utilisateurs;
- l'amélioration constante des mécanismes administratifs, préventifs et d'intervention pour permettre de poser les actions requises pour assurer la sécurité des ressources informationnelles;
- la mise en place d'une veille efficace et préventive pour protéger les ressources informationnelles.

2 Objectifs

La présente politique détermine les responsables et les mesures envisagées afin de maintenir un niveau de sécurité nécessaire à la gestion de l'information de l'Université tout en préservant les principes suivants :

- liberté académique;
- protection de la vie privée et confidentialité;
- éthique, intégrité et responsabilisation.

3 Champ d'application

La présente politique s'applique à l'ensemble des employés et des cadres de l'Université ainsi qu'à toute personne physique ou morale autorisée de façon contractuelle ou autre à utiliser les ressources informationnelles de l'Université.

4 Définitions

Dans cette politique, les expressions suivantes signifient ce qui suit :

« Infonuagique » : Mode d'accès qui permet aux individus et aux organisations d'accéder, par les technologies d'Internet, à un bassin de ressources informatiques externalisées, configurables, et qui sont proposées sous forme de services. Ce mode de livraison de services permet aux consommateurs de s'approvisionner en services de technologies de l'information auprès d'un fournisseur infonuagique de façon automatisée et sur demande[1].

« Plateforme infonuagique personnelle ou publique » : Plateforme infonuagique employée directement par l'utilisateur. Dans ce modèle, aucun contrat ne lie l'Université avec le fournisseur. N'ayant pas fait l'objet d'une analyse préalable, ces plateformes ne sont pas maintenues par l'Université.

« Plateforme infonuagique retenue par l'Université » : Plateforme infonuagique approuvée et soutenue par l'Université. Celle-ci rencontre toutes les exigences de l'Université en matière de sécurité, de fiabilité et de protection des renseignements personnels. L'Université s'assure du respect de ces éléments en concluant un contrat avec le fournisseur de la plateforme.

[1] *Guide de l'infonuagique : Volume 1 – Notions fondamentales, Secrétariat du Conseil du trésor, p. 3.*

« Ressource informationnelle » : Tout équipement relié ou non au réseau, logiciel, système, donnée ou information utilisés pour l'hébergement, le traitement, la diffusion et l'échange d'informations, qu'ils soient la propriété de l'Université ou qu'ils utilisent ou hébergent des actifs dont l'Université est propriétaire, fiduciaire ou dépositaire;

« Utilisateur » : Tout employé ou cadre de l'Université de même que toute personne utilisatrice des ressources informationnelles de l'Université.

5 Cadre juridique

Le cadre juridique de la présente politique est constitué, d'une part, par les lois canadiennes et québécoises en vigueur et, d'autre part, par les politiques et règlements s'appliquant à l'Université. La présente politique découle notamment des principes des législations suivantes :

- *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, chapitre G-1.03);
- *Loi sur les archives* (RLRQ, chapitre A-21.1);
- *Loi sur le droit d'auteur* (L.R.C. (1985), chapitre C-42);
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1).

6 Rôles et responsabilités

6.1 Du vice-président à l'administration

Le vice-président à l'administration est responsable de l'application de la présente politique et, pour ce faire, il peut requérir la collaboration des gestionnaires des autres unités administratives de l'Université, plus particulièrement le Centre de services communs et la Direction des ressources matérielles et immobilières. En cas d'impossibilité d'agir du vice-président à l'administration, le secrétaire général de l'Université sera le responsable de l'application de la présente politique.

Le vice-président à l'administration est autorisé à procéder à toutes les vérifications d'usage qu'il estime nécessaire pour s'assurer du respect de la présente politique. Il est également habilité à mener toute enquête relative à l'utilisation des services informatiques et de télécommunications. Par conséquent, il est entendu qu'il puisse accéder à des données confidentielles lors d'entretiens préventifs ou curatifs, ainsi que dans le cadre des efforts déployés dans le but de maintenir l'intégrité et la confidentialité des systèmes pour lesquels il est responsable.

6.2 Du secrétaire général

Toute personne qui a des motifs sérieux de croire qu'une contravention à la présente politique a été commise doit en saisir, verbalement ou par écrit, le secrétaire général. Elle doit lui fournir tous les renseignements et tous les documents disponibles et pertinents. Ce dernier prend les moyens qu'il jugera appropriés pour effectuer toutes les vérifications requises, incluant celui d'accéder aux données contenues sur les équipements informatiques et de télécommunications.

Dans les cas où le secrétaire général a des motifs de croire qu'une violation à la politique de l'Université ou aux lois et règlements applicables est commise par un utilisateur, il peut prendre les moyens qu'il juge appropriés pour corriger la situation, incluant celui de restreindre ou de bloquer l'accès aux fichiers personnels et au courrier électronique de l'utilisateur sans avis ni délai et sans préjudice à la mise en œuvre des sanctions applicables en vertu de la présente politique.

6.3 De l'Université

L'Université est responsable de fournir les ressources nécessaires à ses utilisateurs afin qu'ils puissent assumer leurs responsabilités quant à la sécurité informatique, et ce, dans un cadre de saine gestion des risques pour l'établissement. Cependant, l'Université ne pourra pas être tenue responsable des pertes, dommages, manques à gagner ou inconvénients qui pourraient être causés à une personne ou à une entité à l'occasion ou en conséquence de l'utilisation des ressources informationnelles de l'Université ou advenant le cas où elle devrait, pour quelque cause que ce soit, diminuer ses services, ou les interrompre, quelle que soit la durée de telles diminutions ou interruptions.

6.4 Des utilisateurs

6.4.1 Codes et authentifiants

Tout utilisateur des ressources informationnelles de l'Université est tenu de préserver la confidentialité de ses codes, mots de passe ou encore de sa carte d'accès.

L'utilisateur est réputé imputable des activités entreprises par le biais de ses codes d'accès (identifiants) et authentifiants. Il est également responsable de restreindre l'accès à des tierces parties aux ordinateurs et autres dispositifs d'accès authentifiés aux réseaux grâce à ses identifiants et authentifiants qu'il aurait divulgués à ces tierces parties.

L'utilisateur doit s'assurer que les authentifiants respectent minimalement les normes institutionnelles de sécurité informatique.

L'utilisateur doit choisir un mot de passe difficile à découvrir et ne pas le communiquer à d'autres personnes. Il ne doit pas également utiliser les fonctions de saisie automatique du mot de passe pour les applications administratives. Enfin, l'Université peut en tout temps mettre en place les mesures suivantes pour assurer l'utilisation optimale des mots de passe :

- Niveau de complexité minimale dans le choix du mot de passe;
- Utilisation d'un mot de passe unique pour chaque système;
- Délai d'inactivité après lequel le système est verrouillé de nouveau;
- Désactivation.

À moins d'une autorisation de l'Université, l'utilisateur ne doit pas poser ou tenter de poser l'un des gestes suivants :

- accès à des données nominatives non requises dans le cadre de son travail;
- prise de connaissance, modification, destruction, déplacement ou divulgation non autorisés des ressources informationnelles;
- lecture, modification ou destruction de tout message, texte, donnée ou logiciel sans l'autorisation de leur propriétaire ou de la ou du responsable des ressources informationnelles concerné;
- décryptage ou décodage de codes ou de clés d'accès, de fichiers ou de mots de passe sans autorisation préalable des responsables de ces ressources;
- utilisation ou transmission à un tiers des clés ou codes d'accès appartenant à autre utilisateur;
- utilisation abusive d'une ressource informationnelle nuisant à son bon fonctionnement;
- contournement des mécanismes de protection des ressources informationnelles;
- non-respect de la réglementation des réseaux externes auxquels l'utilisateur a accès, ni de l'intégrité des systèmes informatiques ainsi accessibles;
- utilisation des ressources informationnelles de l'Université à des fins commerciales non autorisées ou illicites;
- propagation de matériel utilisant un langage injurieux, malveillant, haineux ou discriminatoire, ainsi que de toute forme de harcèlement, de menace ou de diffamation;
- consultation et propagation de matériel pornographique;
- transfert de données de l'Université sur un support externe ou personnel, à moins d'avoir obtenu l'accord de son supérieur immédiat;

- vol de ressources et utilisation malicieuse ou contraire aux lois et règles d'éthique en vigueur.

L'installation, le déplacement, la désinstallation ou l'utilisation d'un logiciel ou d'un équipement de télécommunications personnel (par exemple : routeur, routeur sans fil, équipement RF, etc.) sur le réseau de l'Université doivent être approuvés par l'Université.

Cette approbation a pour but de mieux cerner les besoins du requérant, de l'informer des conséquences de l'utilisation d'un équipement de télécommunications personnel et, au besoin, de lui proposer d'autres solutions dans le cas où l'utilisation d'un de ces équipements pourrait affecter la qualité du service du réseau de télécommunications institutionnel.

6.4.2 Utilisation des services de messagerie électronique

Un utilisateur est responsable de sa messagerie électronique, qui comprend une boîte vocale et une adresse de courriel.

Pour tout message électronique diffusé, l'utilisateur doit s'identifier en tant que signataire du message et préciser, s'il y a lieu, à quel titre il s'exprime.

6.4.3 Comportements interdits

L'utilisateur doit s'assurer que l'utilisation de sa messagerie électronique ou de toute autre messagerie à laquelle il a accès à partir des ressources informationnelles de l'Université (postes de travail, serveurs, téléphones, etc.) respecte la présente politique. À cet effet, les comportements suivants sont interdits :

- utiliser, dans tout courriel diffusé ou dans tout message laissé dans une boîte vocale, un langage injurieux, malveillant, haineux ou discriminatoire, ainsi que toute forme de harcèlement, de menace ou de diffamation;
- capter, stocker, reproduire ou transmettre (au moyen du réseau de télécommunications vers une boîte vocale ou une adresse électronique) du matériel ou un message à caractère illégal;
- se servir de l'adresse de courriel ou de la messagerie électronique à des fins commerciales (annonces publicitaires, pourriels, etc.) ou illicites, ou en faciliter l'utilisation à ces fins;
- avoir recours à un ou des subterfuges ou à d'autres moyens pour transmettre des courriels ou des messages vocaux de façon anonyme ou au nom d'une autre personne.

6.4.4 Accès au courriel pour le personnel de l'Université

L'Université fournit une adresse de courriel à chaque employé. Ce dernier, s'il utilise un poste de travail informatisé, doit consulter régulièrement le contenu de sa boîte de messages pour prendre connaissance des informations qui lui seront transmises par l'Université.

6.4.5 Utilisation à des fins personnelles d'Internet et du courriel

L'utilisation des services informatiques et de télécommunications doit être dédiée à la réalisation des activités de recherche, de gestion, d'administration et de services qui sont offertes par l'Université. Cependant, l'Université tolère, à titre de privilège, l'utilisation occasionnelle à des fins personnelles d'Internet et du courriel dans la mesure où cette utilisation ne cause aucun préjudice à l'Université et qu'elle demeure dans les limites de ce qui est raisonnable. En aucun cas, ces services ne doivent être utilisés par l'utilisateur à des fins commerciales, de publicité ou de promotion d'activités commerciales ou de sollicitation.

Le droit à l'utilisation personnelle n'a pas pour effet d'empêcher l'accès à une ressource informationnelle par une personne autorisée, autre que son utilisateur principal, lorsque cet accès est requis par la nécessité du service et qu'il est autorisé par le supérieur immédiat de l'utilisateur principal ou du secrétaire général.

Dans tous les cas, l'utilisateur principal doit être avisé des accès autorisés, du motif de leur autorisation et de la durée de l'accès par une tierce partie.

6.4.6 Droits de propriété intellectuelle

En tout temps, l'utilisateur doit respecter les droits de propriété intellectuelle, notamment les droits d'auteur des tiers et les ententes contractuelles avec les fournisseurs de contenu, notamment dans le contexte des bibliothèques virtuelles.

La reproduction de logiciels, de progiciels ou de didacticiels n'est autorisée qu'à des fins de copies de sécurité ou selon les normes institutionnelles de la licence d'utilisation la régissant. Il est strictement interdit aux utilisateurs de :

- reproduire ou utiliser toute reproduction illicite d'un logiciel, d'un fichier électronique ou de la documentation qui y est jointe;
- participer directement ou indirectement à la reproduction illicite d'un logiciel ou d'un fichier électronique.

6.4.7 Communication des incidents

Les utilisateurs sont responsables de signaler tout incident de sécurité informatique à leur supérieur immédiat afin de limiter tout dommage aux ressources informationnelles.

Les utilisateurs doivent également collaborer, dans la limite où cette collaboration ne leur portera pas un préjudice personnel, avec les services concernés dans le cadre des exercices d'évaluation de la sécurité informatique et des investigations lors d'incidents de sécurité informatique.

7 Règles et sécurité concernant les plateformes infonuagiques retenues par l'Université

L'Université s'assure par contrat que les plateformes retenues respectent des niveaux de sécurité et de protection de données égaux ou supérieurs à ceux exigés par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.

L'hébergement de données en dehors des serveurs de l'Université représente un enjeu majeur en matière de sécurité. Pour mitiger les risques, l'Université retient les services de fournisseurs réputés dont les serveurs sont situés de préférence au Canada.

Dans ce contexte, il est recommandé d'utiliser les plateformes retenues par l'Université et de respecter les règles suivantes :

- éviter d'emmagasiner sur ces plateformes des documents contenant des renseignements personnels et, lorsque cette solution est inévitable, encrypter les données ou, à tout le moins, en restreindre l'accès à l'aide d'un gestionnaire des droits relatifs à l'information (IRM);
- tout document institutionnel peut être placé sur les plateformes infonuagiques retenues par l'Université, et ce, peu importe que celui-ci soit d'accès public ou restreint. Pour les documents institutionnels à accès restreint, la copie maitresse doit obligatoirement être hébergée sur l'infrastructure de stockage interne de l'Université;
- les documents placés sur les plateformes infonuagiques doivent être partagés exclusivement avec les personnes devant réellement y avoir accès;
- advenant le cas où il est nécessaire de recourir à des plateformes personnelles ou publiques non retenues par l'Université, et ce, dans le cadre des activités professionnelles, l'Université doit approuver préalablement la sélection des outils et prévoir leur installation.

7.1 Mesures de sécurité supplémentaires

L'Université mettra en place des mesures de sécurité supplémentaires dans le cadre de l'utilisation de plateformes infonuagiques. Dans les limites de la technologie et des plans de licence, le recours à une authentification multifacteurs, à des questions de sécurité ou à toute autre méthode permettant d'identifier de manière sans équivoque l'utilisateur est utilisé lorsque possible.

7.2 Sécurité et responsabilité pour les appareils mobiles

Les utilisateurs de plateformes infonuagiques doivent se conformer en tout point à la *Directive pour l'utilisation des appareils mobiles* de l'Université. La section 3 sur la sécurité revêt une importance capitale dans un contexte d'infonuagique.

8 Contrôle et vérification en vertu de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*

En vertu de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*, l'Université doit mettre en place une organisation fonctionnelle de la sécurité de l'information et déterminer les rôles et responsabilités nécessaires à une gouvernance intégrée au plan gouvernemental de gestion et de sécurité de l'information.

Le dirigeant réseau de l'information (DRI) désigné au ministère de l'Éducation et de l'Enseignement supérieur veille à l'application auprès des établissements du réseau de l'éducation des règles de gouvernance et de gestion établies en matière de sécurité de l'information.[2]

En vertu de cette loi, le président de l'Université à titre de dirigeant est responsable de la sécurité de l'information relevant de son autorité. À ce titre, il doit s'assurer du respect des lois et des règles de sécurité de l'information déterminées par le Conseil du trésor, notamment en ce qui a trait à la mise en place de mesures permettant la réduction des risques de sécurité de l'information. Pour le soutenir dans ce rôle, l'Université désigne les personnes suivantes :

[2] *Le DRI est assisté par le responsable organisationnel en sécurité de l'information des réseaux (ROSI-réseau), du coordonnateur organisationnel en gestion des incidents des réseaux (COGI-réseau) et du conseiller organisationnel en sécurité de l'information des réseaux (COSI-réseau).*

8.1 Responsable de la sécurité de l'information (RSI)

Le responsable de la sécurité de l'information (RSI) désigné à l'Université est le vice-président à l'administration qui communique les orientations et les priorités d'intervention gouvernementales en sécurité de l'information.

Le RSI a, en outre, comme responsabilité :

- d'assister le dirigeant de l'Université en ce qui a trait à la détermination des orientations stratégiques et des priorités d'intervention de l'Université;
- d'assurer la coordination et la cohérence des actions de sécurité de l'information menées au sein de l'Université par d'autres intervenants dont les détenteurs de l'information ainsi que les unités responsables des ressources informationnelles, de l'accès à l'information et de la protection des renseignements personnels, de la gestion documentaire, de la sécurité physique et de l'éthique;
- d'assurer la contribution de l'Université au processus de gestion des risques et des incidents de sécurité de l'information à portée gouvernementale;
- de définir et de mettre en œuvre les processus officiels de sécurité de l'information portant sur la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents;
- de s'assurer de la prise en charge des exigences de sécurité de l'information lors de la réalisation de projets de développement ou de l'acquisition de systèmes d'information;
- de coordonner l'élaboration et la mise en œuvre d'un programme officiel et continu de formation et de sensibilisation en matière de sécurité de l'information, dont un registre des incidents.

8.2 Conseiller en sécurité de l'information (CSI)

Le conseiller en sécurité de l'information (CSI) est désigné par le vice-président à l'administration de l'Université. Le CSI apporte son soutien au RSI au niveau tactique, notamment en ce qui a trait à la mise en œuvre des mesures d'atténuation des risques et à la mise en place des processus officiels de sécurité de l'information. Il a notamment comme responsabilité :

- de mettre en œuvre les orientations internes;
- de participer aux négociations des ententes de service et des contrats, et de formuler des recommandations quant à l'intégration de dispositions garantissant le respect des exigences de sécurité de l'information;
- de tenir à jour le registre d'autorité de la sécurité de l'information;

- d'assister les détenteurs de l'information pour ce qui est de la catégorisation de l'information relevant de leur responsabilité et de la réalisation des analyses de risques de sécurité de l'information;
- de contribuer à la mise en œuvre des processus officiels de sécurité de l'information de l'Université;
- d'assurer la gestion et la coordination du plan de continuité des services de l'Université.

8.3 Coordonnateur sectoriel en gestion des incidents (CSGI)

Le coordonnateur sectoriel en gestion des incidents (CSGI) désigné par le vice-président à l'administration de l'Université collabore étroitement avec le RSI et le CSI en leur fournissant le soutien technique nécessaire à l'exercice de leurs responsabilités. Le CSGI a notamment comme responsabilité :

- de contribuer à la mise en place du processus de gestion des incidents de sécurité de l'information de l'Université;
- d'assurer la coordination des membres CERT/AQ[3] qui lui sont rattachés et de mettre en œuvre les stratégies de réaction appropriées;
- de contribuer aux analyses de risques de sécurité de l'information, d'identifier les menaces et les situations de vulnérabilité et de mettre en œuvre les solutions appropriées;
- de contribuer à la mise en œuvre du processus gouvernemental de gestion des incidents de sécurité de l'information;
- d'élaborer et de tenir à jour les guides portant sur la sécurité opérationnelle des systèmes et des réseaux de télécommunications;
- de collaborer étroitement avec le RSI et de lui fournir le soutien technique nécessaire à l'exercice de ses responsabilités.

---

[3] Le réseau d'alerte gouvernemental est animé par le CERT/AQ. Il constitue une plateforme de partage d'information entre les coordonnateurs organisationnels de gestion des incidents désignés en vertu de la Directive sur la sécurité de l'information gouvernementale. Il permet à ses membres :

- *de participer à la coordination des actions en cas d'incidents à portée gouvernementale;*
- *d'accéder à une information pertinente sur les menaces et les vulnérabilités en matière de sécurité de l'information;*
- *d'échanger sur les solutions de sécurité de l'information;*
- *de développer l'expertise en matière de sécurité de l'information et d'accroître la capacité de réaction en cas d'incidents.*

9 Contrôle et vérification par l'Université

Une vérification nominative des renseignements personnels et privés d'un utilisateur ou de son utilisation des ressources informationnelles ne peut être effectuée sans le consentement de cette personne, à moins que le supérieur immédiat ou le secrétaire général n'aient des motifs valables de croire que cette dernière contrevient à l'une ou l'autre des dispositions de la présente politique.

Dans le cas d'une vérification qui impliquerait l'accès à des données privées et confidentielles, que ces données soient l'objet ou non de la vérification, l'Université doit veiller à éviter toute surveillance ou contrôle abusifs. L'Université ne peut vérifier que lorsqu'elle possède des motifs valables de croire qu'un utilisateur manque à ses obligations ou abuse des outils qui lui sont fournis.

10 Sanctions

À la suite de l'enquête menée par le secrétaire général, l'Université peut imposer à l'utilisateur qui contrevient à la présente politique ou commet des actes illégaux, l'une ou plusieurs des sanctions suivantes :

- Annulation du ou des codes d'accès;
- Interdiction permanente ou temporaire d'utiliser en totalité ou en partie les services informatiques et de télécommunications;
- Facturation par l'Université des services obtenus;
- Remboursement à l'Université de toute somme que cette dernière serait appelée à payer à titre de dommages ou pénalités du fait des actes et agissements posés par l'utilisateur, par suite d'une contravention ou de poursuites légales, y compris les frais et honoraires engagés par l'Université dans le cadre de telles poursuites;
- Dans le cas d'un membre du personnel de l'Université, toute autre mesure disciplinaire pouvant aller jusqu'au congédiement.

11 Mesures d'urgence

Afin de préserver l'intégrité des ressources informationnelles, le vice-président à l'administration peut autoriser, après avoir pris les moyens raisonnables pour aviser les responsables ou utilisateurs de ces ressources, les actions suivantes ou exiger qu'elles soient posées :

- interrompre ou révoquer temporairement les services offerts à certains utilisateurs afin de protéger le reste de la communauté;
- intervenir sur une ressource informationnelle suspectée de contrevenir à l'une ou l'autre des dispositions prévues dans cette politique;

- appliquer les différentes fonctions de diagnostic sur les ressources informationnelles;
- prendre les mesures urgentes requises afin de circonscrire la situation.

12 Responsable de l'application et de la mise à jour

Le vice-président à l'administration est responsable de l'application de la présente politique, laquelle est mise à jour au besoin ou révisée tous les trois ans.

13 Adoption et entrée en vigueur

Cette politique* est entrée en vigueur le 14 décembre 2016, date de son adoption par le comité exécutif. Elle a été modifiée le 29 mai 2019.

** Cette politique remplace la Directive concernant la sécurité et l'utilisation des services informatiques et de télécommunications.*