Université du Québec à Rimouski

TITRE :	**POLITIQUE DE SECURITE DE L'INFORMATION**	**C3-D99**
RESPONSABILITÉS :	VICE-RECTORAT AUX RESSOURCES HUMAINES ET A L'ADMINISTRATION SECRETARIAT GENERAL ET VICE-RECTORAT A LA VIE ETUDIANTE	
APPROUVÉE :	CONSEIL D'ADMINISTRATION	RESOLUTION : CA-654-8150 DATE : 16-02-2016
EN VIGUEUR :	16-02-2016	
MODIFICATION :	CA-757-9211 (21-06-2022)	

Note : Le texte que vous consultez est une codification administrative des politiques. La version officielle du présent document est contenue dans les résolutions adoptées par le Conseil d'administration.

TABLE DES MATIÈRES

1. PRÉAMBULE

La présente politique a été adoptée en application de la *Directive sur la sécurité de l'information gouvernementale*[1], de l'article 12. Celle-ci fait obligation aux organismes publics d'adopter et de mettre en œuvre une Politique de sécurité de l'information, de la maintenir à jour et d'en assurer l'application.

L'évolution des pratiques de travail, le partage d'informations, la mobilité des personnes utilisatrices et l'utilisation des technologies deviennent des enjeux majeurs qui accroissent la probabilité que des incidents de sécurité se produisent. Pour y répondre, l'Université du Québec à Rimouski (l'Université) doit faire évoluer son encadrement en matière de sécurité de l'information ainsi que les processus qui en découlent.

Considérant le caractère essentiel de l'information pour la réalisation de sa mission, l'Université reconnait que cette information doit faire l'objet d'une évaluation, d'une utilisation appropriée et d'une protection adéquate en lien avec la disponibilité, l'intégrité et la confidentialité

2. DÉFINITIONS

Actif informationnel : Systèmes d'information, réseau de télécommunication, infrastructure technologique ou un ensemble de ces éléments contenant un document. Est également considéré comme un actif informationnel l'information regroupée dans un système d'information ou un support papier contenant un document.

Document : Ensemble constitué d'informations portées par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcrit sous l'une de ses formes ou en un autre système de symboles.

Est aussi considéré comme document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite.

Support : Moyen de conservation et de diffusion d'information autre qu'un système d'information. Un support peut être numérique (clé USB, disque compact, bande de copie, disque externe, vidéo, etc.) ou papier.

Système d'information : Ensemble organisé de ressources matérielles et logiciels permettant d'acquérir, de conserver, de traiter, et de diffuser les éléments d'information.

Confidentialité : Propriété d'une information de n'être accessible qu'aux personnes utilisatrices 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, 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.

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

[1] Directive sur la sécurité de l'information gouvernementale - Secrétariat du Conseil du trésor

Intégrité : Propriété associée à une information de ne subir aucune altération ou destruction sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité. L'intégrité fait référence à l'exactitude et à la complétude.

3. CADRE LÉGAL ET ADMINISTRATIF

La *Politique de sécurité de l'information* s'inscrit principalement dans un contexte régi par :

- la *Loi sur l'Université du Québec* (RLRQ, ch. U-1);
- la *Charte des droits et libertés de la personne* (RLRQ, ch. C-12);
- le *Code civil du Québec* (RLRQ,, ch. CCQ-1991);
- la *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics*;
- la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, ch. G-1.03);
- la *Loi concernant le cadre juridique des technologies et l'information* (RLRQ, chapitre C-1.1);
- la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1);
- la *Loi sur les archives* (RLRQ, chapitre A-21.1);
- la *Loi canadienne sur les droits de la personne* (LRC, 1985, chapitre H-6);
- le *Code criminel* (LRC, 1985, chapitre C-46);
- la *Loi sur le droit d'auteur* (LRC, 1985, chapitre C-42);
- le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1, r. 02);
- la *Directive sur la sécurité de l'information gouvernementale*;
- le Règlement 15 : *Registres officiels et documentation administrative de l'Université*.

4. OBJECTIF DE LA POLITIQUE

La présente politique a pour objectif d'affirmer l'engagement de l'Université de s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, quel que soit son support ou son moyen de communication. Plus précisément, il s'agit d'assurer, tout au long du cycle de vie de l'information, sa disponibilité, son intégrité et sa confidentialité.

5. CHAMP D'APPLICATION

La présente politique s'adresse à toutes les personnes utilisatrices des actifs informationnels de l'Université, c'est-à-dire, sans s'y limiter, le personnel cadre, les professeures et professeurs, les personnes chargées de cours, le personnel administratif et de soutien, les étudiantes et étudiants de même que toute personne physique ou morale qui à titre de personne consultante, de partenaire ou de personne agissant à titre de fournisseur de services.

Les actifs informationnels visés sont ceux que l'Université détient dans l'exercice de ses activités, que sa détention soit assurée par elle-même ou par un tiers.

6. ÉNONCÉS DE PRINCIPES GÉNÉRAUX

6.1 Protection de l'information

a) L'Université adhère aux orientations et objectifs stratégiques gouvernementaux en matière de sécurité de l'information et s'engage à ce que les pratiques et les solutions retenues en la matière correspondent, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées, tant à l'échelle nationale qu'à l'échelle internationale.

b) L'Université reconnait que les actifs informationnels qu'elle détient sont essentiels à ses activités courantes et, de ce fait, qu'ils doivent faire l'objet d'une évaluation constante, d'une utilisation appropriée et d'une protection adéquate. Le niveau de protection, dont les actifs informationnels doivent faire l'objet, est établi en fonction de leur importance, de leur confidentialité et des risques d'incident, d'erreur et de malveillance auxquels ils sont exposés.

c) La sécurité des actifs informationnels est soutenue par une démarche éthique visant à assurer la régulation des conduites et la responsabilisation individuelle.

6.2 Protection des renseignements confidentiels

Toute information confidentielle doit être préservée de toute divulgation, de tout accès ou de toute utilisation non autorisée.

Sont notamment considérés comme confidentiels, au sens de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, les renseignements personnels ainsi que tout renseignement dont la divulgation aurait des incidences, notamment sur les relations intergouvernementales, les négociations entre organismes publics, l'économie, les tiers relativement à leurs renseignements industriels, financiers, commerciaux, scientifiques ou techniques, l'administration de la justice et la sécurité publique, les décisions administratives ou politiques et la vérification.

Toute autre information peut être confidentielle et visée par la présente politique si elle est désignée comme tel par les parties concernées, notamment en matière contractuelle.

6.3 Sensibilisation et formation

L'Université s'engage, sur une base régulière, à sensibiliser et à former les personnes utilisatrices à la sécurité des actifs informationnels, aux conséquences d'une atteinte à leur sécurité ainsi qu'à leurs rôles et obligations en la matière.

6.4 Droit de regard

L'Université exerce, en conformité avec la législation et la réglementation en vigueur, un droit de regard de ses actifs informationnels, notamment de contrôle et à la vérification de leurs usages.

7. OBLIGATIONS DES PERSONNES INTERVENANTES CLÉS EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION

La présente politique fixe les obligations en matière de sécurité de l'information attribuées aux personnes intervenantes clés en matière de sécurité de l'information, soit, à la rectrice ou au recteur, aux personnes responsables de la sécurité de l'information, détentrices d'information, cadres et

utilisatrices. La rectrice ou le recteur est la première personne responsable de la sécurité de l'information relevant de la juridiction de l'Université.

a) La personne responsable organisationnelle de la sécurité de l'information (ROSI) assiste la rectrice ou le recteur dans la détermination des orientations stratégiques et des priorités d'intervention.

b) La personne détentrice de l'information est la personne cadre désignée par la personne ROSI dont le rôle est entre autres de s'assurer de la sécurité de l'information et des ressources qui la sous-tendent, relevant de la responsabilité de son unité administrative.

c) Toute personne cadre est chargée de la mise en œuvre des dispositions de la présente politique auprès des membres du personnel relevant de son autorité.

Les structures internes de coordination et de concertation en matière de sécurité de l'information ainsi que les rôles et les responsabilités détaillés de toutes les personnes intervenantes sont définis dans le cadre de gestion de la sécurité de l'information, en complément à la présente politique.

8. OBLIGATIONS DES PERSONNES UTILISATRICES

Une personne utilisatrice est toute personne de l'Université de quelque catégorie d'emploi, de statut d'employé ainsi que toute personne morale ou physique qui, par engagement contractuel ou autrement, utilise un actif informationnel de l'Université ou y a accès.

Toute personne utilisatrice a l'obligation de protéger les actifs informationnels mis à sa disposition par l'Université. À cette fin, elle doit :

a) prendre connaissance de la présente politique, du cadre de gestion sur la sécurité de l'information, des directives, des procédures et autres lignes de conduite en découlant, y adhérer et prendre l'engagement de s'y conformer;

b) utiliser les actifs informationnels en conformité avec les accès qui lui sont attribués et en se limitant aux fins auxquelles ils sont destinés;

c) respecter les mesures de sécurité visant à protéger les systèmes d'information et ne pas modifier leur configuration ou les désactiver;

d) se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels des droits de propriété intellectuelle pourraient exister;

e) signaler immédiatement tout acte dont elle a connaissance, susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels de l'Université.

9. SANCTIONS

Lorsqu'une personne utilisatrice contrevient à la présente politique, au cadre de gestion de la sécurité de l'information ou aux directives et procédures en découlant, elle s'expose à des mesures disciplinaires, administratives ou légales, en fonction de la gravité de son geste. Ces mesures peuvent inclure la suspension des privilèges, la réprimande, la suspension, le congédiement ou autre, et ce, conformément aux dispositions des conventions collectives, des protocoles, des ententes ou des contrats applicables selon le cas.

L'Université peut transmettre à toute autorité judiciaire les renseignements colligés qui la portent à croire qu'une infraction à tout règlement ou loi en vigueur a été commise.

10. DISPOSITIONS FINALES

a) La présente politique entre en vigueur à la date de son adoption par le Conseil d'administration de l'Université du Québec à Rimouski.

b) La présente politique doit être révisée lors de changements qui pourraient l'affecter.

c) La présente politique est complétée par le cadre de gestion de la sécurité de l'information et les obligations qui en découlent sont précisées dans des directives et des procédures.