POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION

Instance compétente : Conseil d'administration

Responsable de l'application : Vice-recteur à l'administration et aux finances

Date d'entrée en vigueur : 17 juin 2019
Adoption : 17 juin 2019 (2019-CA664-04.01.03-R7319)

TABLE DES MATIÈRES

1. PRÉAMBULE

Dans l'exercice de ses fonctions, l'Université du Québec à Trois-Rivières (UQTR) recueille, utilise, produit, communique et conserve une quantité croissante d'information que ce soit sur support papier ou technologique.

À l'instar d'autres organismes, l'UQTR fait face à un nombre grandissant de menaces pouvant porter atteinte à la confidentialité, l'intégrité et la disponibilité de cette information. Ces menaces, dont la nature est en constante évolution, comprennent, entre autres, le vol de renseignements personnels, le piratage, l'hameçonnage, la fraude, l'espionnage, l'accès non autorisé à l'information, les défaillances techniques, les événements naturels et les erreurs humaines.

L'UQTR considère qu'il est crucial de poursuivre et d'accentuer ses efforts pour protéger son information et les ressources qui la sous-tendent et à cet égard, de se doter d'un cadre normatif spécifique et d'une gouvernance forte et intégrée en matière de sécurité de l'information.

C'est dans ce contexte que l'UQTR adopte la présente politique.

2. OBJET

La présente politique définit les objectifs et principes ainsi que la gouvernance de l'UQTR en matière de sécurité de l'information.

3. CHAMP D'APPLICATION

Cette politique s'applique à l'information que détient l'UQTR dans l'exercice de ses fonctions, que la conservation de cette information soit assurée par elle-même ou un tiers.

Elle s'applique à tous les utilisateurs de cette information.

4. CADRE JURIDIQUE

La présente politique est adoptée en vertu de l'article 7 de la Directive sur la sécurité de l'information gouvernementale (Décret 7-2014) découlant de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ c. G-1.03). Elle s'appuie en outre sur le cadre normatif gouvernemental suivant :

- Le Cadre gouvernemental de gestion de la sécurité de l'information;
- Le Cadre de gestion des risques et des incidents à portée gouvernementale en sécurité de l'information ;

- L'Approche stratégique gouvernementale en sécurité de l'information 2014-2017;

La présente politique est également associée aux lois et aux documents normatifs de l'UQTR suivants :

- Le Code civil du Québec (RLRQ c. CCQ-1991, art. 3, 35 à 37);
- La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1);
- La Loi concernant le cadre juridique des technologies de l'information (RLRQ, c. C-1.1);
- La Loi sur les archives (RLRQ c. A-21.1);
- La Politique portant sur les utilisations des technologies de l'information et des communications de l'UQTR;
- Le Règlement établissant les politiques et les normes relatives à la confidentialité, à l'accès aux dossiers des étudiants et à la conservation de ces dossiers à l'UQTR;
- La Politique de gestion des documents actifs, semi-actifs et inactifs de l'UQTR;
- Le Règlement relatif à la sécurité sur le campus;
- Le Code d'éthique et de déontologie des membres du personnel;
- La Politique de gestion des risques.

5. DÉFINITIONS

« CERT/AQ » : Désigne l'équipe de réponse aux incidents de sécurité de l'information de l'administration québécoise à portée gouvernementale.

« Communauté universitaire » : Les étudiants, les membres du personnel, les membres de toute instance ou de tout comité, les professeurs associés ou invités, les membres d'une unité de recherche ainsi que les stagiaires postdoctoraux et autres stagiaires de l'UQTR.

« Détenteur de l'information » : Les cadres désignés par le vice-recteur à l'administration et aux finances, lesquels ont la responsabilité de s'assurer de la sécurité de l'information, incluant des ressources qui la sous-tendent, relevant de l'unité administrative dont ils assument la direction.

« Document » : Un ensemble constitué d'information portée par un support papier ou technologique. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et 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 transcrits sous l'une de ces formes ou en un autre système de symboles. Est assimilée au 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.[1]

« Information » : L'information que détient l'UQTR consignée dans un document, quel qu'en soit le support, que la conservation de cette information soit assurée par elle-même ou un tiers.

« Incident de sécurité de l'information à portée gouvernementale » : Conséquence observable de la concrétisation d'un risque de sécurité de l'information à portée gouvernementale, nécessitant une intervention concertée au plan gouvernemental.

« Registre d'autorité de la sécurité de l'information » : Registre dans lequel sont notamment consignés les noms des détenteurs de l'information, les systèmes qui leur sont assignés ainsi que les rôles et les responsabilités des principaux intervenants en sécurité de l'information.

« Registre d'incident » : Registre dans lequel sont consignés la nature d'un incident de sécurité de l'information, l'impact, les mesures prises pour le rétablissement à la normale et le suivi.

« Risque de sécurité de l'information à portée gouvernementale » : Risque d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information et qui peut avoir des conséquences sur la prestation de services à la population, sur la vie, la santé ou le bien-être des personnes, sur le respect de leurs droits fondamentaux à la protection des renseignements personnels qui les concernent et au respect de leur vie privée, sur l'image du gouvernement ou sur la prestation de services fournie par d'autres organismes publics.

« Utilisateur » : Un membre de la communauté universitaire de même que tout tiers qui accède à l'information ou l'utilise.

6. OBJECTIFS ET PRINCIPES DIRECTEURS DE LA SÉCURITÉ DE L'INFORMATION

6.1 Objectifs

L'UQTR met en place des mesures de sécurité proportionnelles à la valeur de l'information à protéger. Ces mesures sont déterminées en fonction des risques, de leur probabilité d'occurrence et de leurs conséquences. Ces mesures visent plus particulièrement à :

[1] Source : Directive sur la sécurité de l'information gouvernementale (Décret 7-2014, a.3).

a) Assurer la disponibilité de l'information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise par une personne autorisée;

b) Assurer l'intégrité de l'information de manière à ce que celle-ci ne soit pas détruite ou altérée de quelque façon sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues;

c) Limiter la divulgation de l'information aux seules personnes autorisées à en prendre connaissance, assurant ainsi une stricte confidentialité;

d) Permettre de confirmer l'identité d'une personne ou l'identification d'un document ou d'un dispositif;

e) Se prémunir contre le refus d'une personne de reconnaître sa responsabilité à l'égard d'un document ou d'un autre objet, dont un dispositif d'identification avec lequel elle est en lien.

6.2 Principes directeurs

L'UQTR assure la sécurité de l'information conformément aux principes directeurs suivants :

a) Responsabilité et imputabilité : l'efficacité des mesures de sécurité de l'information exige l'attribution claire des responsabilités à tous les niveaux de l'organisation et la mise en place d'un processus de gestion interne de la sécurité permettant une reddition de comptes adéquate;

b) 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;

c) 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;

d) Éthique : le processus de gestion de la sécurité de l'information doit être soutenu par une démarche d'éthique visant à assurer la régulation des conduites et la responsabilisation individuelle.

7. GOUVERNANCE DE LA SÉCURITÉ DE L'INFORMATION

7.1 Les principaux intervenants de la sécurité de l'information

7.1.1 Le conseil d'administration

Le conseil d'administration est le dirigeant de l'organisme pour l'application de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement. À ce titre, il :

a) Adopte la présente politique et la maintient à jour, conformément à la Directive sur la sécurité de l'information gouvernementale;

b) Confie au vice-recteur à l'administration et aux finances et au Responsable de la sécurité de l'information (RSI) les responsabilités dévolues au dirigeant de l'organisme en vertu de la Directive sur la sécurité de l'information et du Cadre gouvernemental de gestion de la sécurité de l'information, le tout conformément aux dispositions prévues à la présente politique;

c) Reçoit annuellement le bilan des réalisations en matière de sécurité de l'information.

7.1.2 Le comité d'audit

Le comité d'audit exerce les rôles et les responsabilités qui lui sont confiés dans la Politique sur la gestion des risques.

7.1.3 Le vice-recteur à l'administration et aux finances

Le vice-recteur à l'administration et aux finances agit comme premier responsable de la sécurité de l'information. Principalement, il :

a) S'assure du respect du cadre législatif et normatif de la sécurité de l'information;

b) S'assure de l'application de la présente politique et de sa mise à jour;

c) Approuve les directives et procédures pour appuyer la présente politique. Il s'assure de leur application et de leur mise à jour;

d) Désigne les détenteurs de l'information;

e) Approuve les cadres de gestion, dont un cadre de gestion définissant les rôles et responsabilités des intervenants en sécurité de l'information. Il s'assure de leur application et de leur mise à jour;

f) Approuve les orientations stratégiques, les plans d'action et les priorités d'intervention et s'assure de leur suivi;

g) Approuve un programme formel et continu de formation et de sensibilisation du personnel. Il s'assure de son application et de sa mise à jour;

h) Reçoit et analyse les recommandations du comité de la sécurité de l'information et s'assure du suivi auprès des personnes concernées, le cas échéant;

i) Présente annuellement au conseil d'administration un bilan des réalisations en matière de sécurité de l'information.

7.1.4 Le responsable de la sécurité de l'information (RSI)

Le directeur du Service des technologies de l'information assume le rôle de responsable de la sécurité de l'information (RSI). Principalement, il :

a) Agit à titre de répondant de l'UQTR auprès du dirigeant réseau de l'information (DRI) du ministère de l'Éducation et de l'Enseignement supérieur;

b) Désigne le coordonnateur sectoriel de gestion des incidents (CSGI);

c) Conseille la haute direction en matière de sécurité de l'information;

d) Assiste et conseille le vice-recteur à l'administration et aux finances relativement à la détermination des orientations stratégiques, des plans d'action, des priorités d'intervention, des cadres de gestion et des directives et procédures en matière de sécurité de l'information;

e) Soumet à la consultation du comité de la sécurité de l'information, les orientations stratégiques, les plans d'action, les priorités d'intervention, les modifications à la présente

politique, les directives, les procédures, les cadres de gestion, ainsi que tout événement ayant mis ou qui aurait pu mettre en péril la sécurité de l'information;

f) Définit et met en œuvre les processus de sécurité de l'information portant sur la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents;

g) Assure la coordination et la cohérence des actions de la sécurité de l'information menées au sein de l'établissement;

h) Soutient les unités administratives et académiques ainsi que les détenteurs de l'information dans la prise en charge des exigences de sécurité de l'information;

i) S'assure de la réalisation d'un audit de sécurité de l'information, selon une périodicité bisannuelle ou à la suite d'un changement majeur susceptible d'avoir des conséquences sur la sécurité de l'information, et en dégage les priorités d'intervention ainsi que les échéanciers afférents;

j) S'assure de la réalisation de tests d'intrusion et de vulnérabilité, annuellement ou à la suite d'un changement majeur susceptible d'avoir des conséquences sur la sécurité de l'information, et en dégage les priorités d'intervention et les échéanciers afférents;

k) Dépose au dirigeant réseau de l'information (DRI) du ministère de l'Éducation et de l'Enseignement supérieur, selon les modalités, le format et la périodicité fixés, une planification des actions de sécurité de l'information et un bilan de sécurité de l'information;

l) S'assure que les ententes conclues avec les prestataires de services, les partenaires et les mandataires, stipulent des clauses garantissant le respect des exigences de sécurité de l'information;

m) Favorise l'utilisation des services communs de sécurité de l'information déterminés par le Conseil du trésor;

n) S'assure 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;

o) Coordonne l'élaboration et la mise en œuvre d'un programme formel et continu de formation et de sensibilisation du personnel en matière de sécurité de l'information;

p) Met en place et maintient à jour un Registre d'autorité de la sécurité de l'information;

q) Déclare au dirigeant réseau de l'information (DRI) du ministère de l'Éducation et de l'Enseignement supérieur, selon les modalités fixées par ce dernier, les risques de sécurité de l'information à portée gouvernementale;

r) Déclare au CERT/AQ, selon les modalités fixées par ce dernier, les incidents de sécurité de l'information à portée gouvernementale;

s) Maintient un registre des incidents et gère le processus hiérarchique et de résolution de problème dans ce domaine;

t) Effectue le suivi des observations et des recommandations en matière de sécurité de l'information formulées par les auditeurs;

u) Présente annuellement au vice-recteur à l'administration et aux finances et au comité de la sécurité de l'information le bilan des réalisations en matière de sécurité de l'information.

7.1.5 Le coordonnateur sectoriel de gestion des incidents (CSGI)

Le coordonnateur sectoriel de gestion des incidents (CSGI) collabore étroitement avec le responsable de la sécurité de l'information (RSI) et lui fournit le soutien technique nécessaire pour qu'il puisse s'acquitter de ses responsabilités. Principalement, il :

a) Contribue à la mise en place des processus de la sécurité de l'information;

b) Contribue aux analyses de risques de sécurité de l'information, identifie les menaces et les situations de vulnérabilité et met en œuvre les solutions appropriées;

c) Coordonne la gestion des incidents de la sécurité de l'information;

d) Rapporte les incidents de la sécurité de l'information au coordonnateur organisationnel réseau de gestion des incidents du ministère de l'Éducation et de l'Enseignement supérieur (COGI - réseau);

e) Élabore et tient à jour les guides portant sur la sécurité opérationnelle des systèmes et des réseaux de télécommunications ;

f) Contribue à l'auto-évaluation de la sécurité des systèmes informatiques et des réseaux informatiques, notamment par des exercices d'audit de sécurité et des tests d'intrusion aux systèmes jugés à risque;

g) Maintient une veille continue sur les risques, les menaces et les vulnérabilités;

h) Établit des liens avec les autres coordonnateurs sectoriels de gestion des incidents (CSGI) du réseau des établissements d'enseignement supérieur afin de privilégier le partage d'expertise et des éléments tactiques opérationnels à élaborer et à mettre en œuvre;

7.2 Le comité de la sécurité de l'information

Le comité de la sécurité de l'information constitué en vertu de la présente politique est la principale instance de concertation en matière de sécurité de l'information. Plus particulièrement, il :

a) Examine les orientations stratégiques, les plans d'action, les priorités d'intervention, les modifications à la présente politique, les directives, les procédures et les cadres de gestion ainsi que les projets en sécurité de l'information qui lui sont soumis et formule à cet égard ses recommandations au vice-recteur à l'administration et aux finances;

b) Analyse les événements ayant mis ou qui auraient pu mettre en péril la sécurité de l'information et formule à cet égard ses recommandations au vice-recteur à l'administration et aux finances.

Ce comité comprend :

a) Le responsable de la sécurité de l'information (RSI) qui le préside;
b) L'adjoint au vice-recteur à l'administration et aux finances, à titre de coordonnateur de la gestion des risques;

c) Le directeur du Service des finances ou son représentant;
d) Le directeur du Service des ressources humaines ou son représentant;
e) Le doyen de la gestion académique des affaires professorales ou son représentant;
f) Le registraire ou son représentant;
g) Le responsable de la gestion documentaire du Service de la gestion des documents et des archives;
h) Le secrétaire général, à titre de responsable de l'accès aux documents des organismes publics et sur la protection des renseignements personnels, ou son représentant.

7.3 Le comité de crise de la sécurité de l'information

En cas d'incident critique de sécurité de l'information, le comité de gestion des mesures d'urgence (CGMU) constitue le comité de crise de la sécurité de l'information. Ce comité est l'instance décisionnelle appelée à intervenir, notamment lorsque les tentatives de rétablissement des activités n'ont pas apporté les résultats escomptés ou qu'aucune mesure palliative n'a pu assurer la continuité ou la reprise rapide des services. Ce comité est composé des membres du comité de gestion des mesures d'urgence (CGMU) ainsi que du responsable de la sécurité de l'information (RSI). Il comprend donc:

a) Le recteur, qui en assume la présidence;
b) Les vice-recteurs;
c) Le directeur du Bureau du recteur;
d) Le secrétaire général;
e) Le directeur du Service des communications, du recrutement et Bureau des diplômés;
f) Le directeur du Service de la protection publique et de la santé et sécurité au travail;
g) Le responsable de la sécurité de l'information (RSI).

Ce comité peut s'adjoindre toute autre personne dans le cadre de ses prises de décisions.

8. OBLIGATIONS DES UTILISATEURS

La responsabilité de la sécurité de l'information incombe à tous les utilisateurs. Chacun d'eux doit :

a) Se conformer à la présente politique et aux directives, procédures, cadres de gestion et autres lignes de conduite en découlant;

b) Respecter les mesures de sécurité de l'information mises en place, ne pas les contourner, ni les modifier ou les désactiver;

c) Signaler au responsable de la sécurité de l'information (RSI) toute situation susceptible de constituer une violation à la présente politique ou tout incident susceptible de menacer la sécurité de l'information.

9. SANCTIONS

Lorsqu'un utilisateur contrevient à la présente politique, aux directives, procédures, cadres de gestion ou autres lignes de conduite en découlant, il s'expose à des sanctions déterminées selon les processus prévus aux conventions collectives, protocoles, ententes et documents normatifs de l'UQTR.

10. RESPONSABLE DE L'APPLICATION DE LA POLITIQUE

Le vice-recteur à l'administration et aux finances est responsable de l'application de la présente politique.

11. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur au moment de son adoption par le conseil d'administration.

12. MISE À JOUR

La présente politique est mise à jour tous les 5 ans.

Références :

2019-CA664-04.01.03-R7319, 17 juin 2019