CÉGEP de La Pocatière
Centre d'études collégiales de Montmagny

Cahier de gestion

POL-6501-2017

Politique sur la sécurité de l'information

Type de document :

☐ Règlement ☒ Politique ☐ Directive ☐ Procédure

Instance d'approbation :

☒ Conseil d'administration ☐ Comité de direction

Politique adoptée le 14 juin 2017.

Mise à jour le :

L'utilisation des termes génériques masculins permet d'alléger le texte.

TABLE DES MATIÈRES

1. PRÉAMBULE

Cette politique permet au cégep de La Pocatière d'accomplir sa mission, de préserver sa réputation, de respecter les lois et de réduire les risques en protégeant l'information qu'il a créée ou reçue; dont il est le gardien. Cette information est multiple et diversifiée. Elle consiste en des renseignements personnels d'étudiants et de membres du personnel, en de l'information professionnelle sujette à des droits de propriétés intellectuelles (enseignants et chercheurs) et, finalement, en de l'information stratégique ou opérationnelle pour l'administration du cégep.

Notre cégep, faisant partie du réseau de l'enseignement supérieur, a une image publique et est une cible potentielle pour du piratage.

Dans ce contexte, l'entrée en vigueur de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, chapitre. G-1.03) et de la Directive sur la sécurité de l'information gouvernementale (une directive du Conseil du trésor du Québec applicable au cégep) crée des obligations aux établissements collégiaux en leur qualité d'organismes publics. Ainsi, la Directive sur la sécurité de l'information gouvernementale oblige le cégep à adopter, à mettre en œuvre, à maintenir à jour et à assurer l'application d'une politique de sécurité de l'information – dont les principales modalités sont définies dans la directive gouvernementale – en ayant recours, notamment à des processus formels de sécurité de l'information qui permettent d'assurer la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents.

Cadre légal et administratif

- la Charte des droits et libertés de la personne (LRQ, chapitre C-12);
- le Code civil du Québec (LQ, 1991, chapitre 64);
- 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 (LRQ, chapitre G-1.03);
- la Loi concernant le cadre juridique des technologies de l'information (LRQ, chapitre C- 1.1);
- la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LRQ, chapitre A-2.1);
- la Loi sur les archives (LRQ, chapitre A-21.1);
- le Code criminel (LRC, 1985, chapitre C-46);
- le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r. 2);
- la Directive sur la sécurité de l'information gouvernementale;

- la Loi sur le droit d'auteur (LRC, 1985, chapitre C-42).
- la Politique régissant l'utilisation des médias sociaux;
- la Directive relative à la gestion documentaire;
- la Directive relative à la protection des renseignements personnels.

2. DÉFINITIONS

Actif informationnel

Une information, une banque d'information, un système ou un support d'information, un document, une technologie de l'information, une installation ou un ensemble de ces éléments acquis ou constitué par le cégep habituellement accessible ou utilisable avec un dispositif des technologies de l'information (logiciels, progiciels, didacticiels, banques de données et d'informations textuelles, sonores, symboliques ou visuelles placées dans un équipement ou sur un média informatique, système de courrier électronique et système de messagerie vocale). Cela inclut l'information ainsi que les supports tangibles ou intangibles permettant son traitement, sa transmission ou sa conservation aux fins d'utilisation prévue (ordinateurs fixes ou portables, tablettes électroniques, téléphones intelligents, etc.) de même que l'information fixée sur un support analogique, dont le papier.

Catégorisation

Le processus d'assignation d'une valeur à certaines caractéristiques d'une information, qualifiant le degré de sensibilité de cette information et, conséquemment, la protection à lui accorder en termes de disponibilité, d'intégrité et de confidentialité.

Détenteur

Une personne qui a la garde d'une partie ou de la totalité d'un actif informationnel ou de plusieurs actifs informationnels du cégep.

Détenteur de l'information

Un employé désigné par son organisme public, appartenant à la classe d'emploi de niveau-cadre ou à une classe d'emploi de niveau supérieur, et dont le rôle est, notamment, de s'assurer de la sécurité de l'information et des ressources qui la sous-tendent, relevant de la responsabilité de son service. Le terme « détenteur de processus d'affaires » est utilisé lorsque ce rôle se limite à un processus d'affaire déterminé.

Document

Un ensemble constitué d'information portée par un support. 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.

Incident de sécurité

La conséquence observable de la concrétisation d'un risque de sécurité de l'information à portée gouvernementale, nécessitant une intervention concertée au plan gouvernemental.

Information

Un renseignement consigné sur un support quelconque pour être conservé, traité ou communiqué comme élément de connaissance.

Mesure de sécurité de l'information

Un moyen concret assurant partiellement ou totalement la protection d'information du cégep contre un ou plusieurs risques (panne majeure du réseau informatique ou des serveurs institutionnels, acte involontaire, acte malveillant tel que l'intrusion dans un système informatique, etc.) et dont la mise en œuvre vise à amoindrir la probabilité de survenance de ces risques ou à réduire les pertes qui en résultent.

3. OBJECTIFS

La présente politique a pour objectif d'affirmer l'engagement du cégep à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, quels que soient son support ou ses moyens de communication. Plus précisément le cégep doit veiller à :

- 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 ni détruite ni altérée d'aucune 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, surtout si elle constitue des renseignements personnels.

Par conséquent, le cégep met en place cette politique dans le but d'orienter et de déterminer sa vision, qui sera détaillée par le cadre de gestion de la sécurité de l'information de l'institution.

Le cadre de gestion de la sécurité de l'information renforce les systèmes de contrôles internes en offrant une assurance raisonnable de conformité à l'égard des lois et directives gouvernementales, ainsi qu'aux autres besoins du cégep en matière de réduction du risque associé à la protection de l'information.

4. CHAMPS D'APPLICATIONS

La présente politique s'adresse aux utilisateurs de l'information, c'est-à-dire tout le personnel, à toute personne physique ou morale qui, à titre d'employé, de consultant, de partenaire, de fournisseur, d'étudiant ou de public utilise les actifs informationnels du cégep.

L'information visée est celle que le cégep détient dans le cadre de ses activités, que sa conservation soit assurée par lui-même ou par un tiers.

Tous les supports, incluant le papier, sont concernés.

5. PRINCIPES DIRECTEURS

Les principes directeurs qui guident les actions du cégep en matière de sécurité de l'informations ont les suivants :

a) s'assurer de bien connaître l'information à protéger, en identifier les responsables et leurs caractéristiques de sécurité (principe qui confirme l'importance de maintenir à jour l'inventaire des actifs informationnels);

b) s'appuyer sur les normes internationales pertinentes afin de favoriser le déploiement des meilleures pratiques et de recourir à des barèmes de comparaison avec les organismes ou établissements similaires;

c) adhérer à une approche basée sur le risque acceptable (la mise en place du cadre de gestion étant un moyen d'ajuster le risque, par une combinaison de mesures raisonnables mises en place pour garantir la sécurité de l'information, à un coût proportionnel à la sensibilité de l'information et aux effets potentiels);

d) reconnaître l'importance de la politique de sécurité de l'information, du cadre de gestion de la sécurité de l'information qui doit être articulé par une équipe compétente et suffisante en nombre (cette équipe devant définir, mettre en place, opérer et ajuster la gestion de la sécurité de l'information);

e) protéger rigoureusement les renseignements personnels ainsi que toute autre information confidentielle;

f) reconnaître que l'environnement technologique est en changement constant et interconnecté avec le monde (en mettant en place une gestion de la sécurité de l'information qui s'adapte à ces changements);

g) reconnaître l'importance d'évaluer régulièrement les risques, de mettre en place des mesures proactives de sécurité et des méthodes de détection d'usage abusif ou inapproprié de l'information, de définir des actions d'éradication des menaces ou de recouvrement des activités compromises;

h) protéger l'information tout au long de son cycle de vie, c'est-à-dire de son acquisition ou de sa création jusqu'à sa destruction (le niveau de sécurité pouvant varier au cours du cycle de vie du document);

i) adhérer aux principes de partage des meilleures pratiques et de l'information opérationnelle en matière de la sécurité de l'information avec le réseau de l'éducation et organismes publics;

j) adhérer à une démarche éthique visant à assurer la régulation des conduites et la responsabilisation individuelle (chaque individu qui a accès à l'information étant responsable de respecter les critères de confidentialité, de disponibilité et d'intégrité de celle-ci;

k) s'assurer que chaque employé doit avoir accès au minimum d'information requis pour accomplir ses tâches normales;

l) communiquer de façon transparente au sujet des menaces pouvant affecter les actifs informationnels, afin que chacun puisse comprendre l'importance d'appliquer la sécurité comme on le demande, être informé de telle sorte qu'il puisse reconnaître les incidents de sécurité et agir en conséquence;

m) mettre en place un plan de continuité des affaires en vue de rétablir les services essentiels à sa clientèle, selon un temps prévu.

6. MODALITÉS D'APPLICATION

Cadre de gestion

L'efficacité des mesures de sécurité de l'information exige l'attribution claire des rôles et des responsabilités aux différents acteurs du cégep par la mise en place d'un cadre de gestion de la sécurité permettant notamment une reddition de comptes adéquate

Les pratiques et solutions retenues en matière de sécurité de l'information doivent être remises en question de manière périodique dans le but de tenir compte non seulement

des changements juridiques, organisationnels, technologiques, physiques et environnementaux, mais aussi de l'évolution de menaces et des risques.

La politique de sécurité de l'information du cégep s'articule autour de trois axes fondamentaux de gestion. Ces axes sont la gestion des accès, la gestion des risques et la gestion des incidents.

Gestion des accès

La gestion des accès doit être encadrée et contrôlée pour faire en sorte que l'accès, la divulgation et l'utilisation de l'information soient strictement réservés aux personnes autorisées. Ces mesures sont prises dans le dessein de protéger l'intégrité et la confidentialité des données et des renseignements personnels.

L'efficacité des mesures de sécurité de l'information repose sur l'attribution de responsabilité et une imputabilité des personnes, à tous les niveaux de personnel du cégep.

Gestion des risques

Une catégorisation des actifs informationnels à jour soutient l'analyse de risques en permettant de connaître la valeur de l'information à protéger.

L'analyse de risques guide également l'acquisition, le développement et l'exploitation des systèmes d'information, en spécifiant les mesures de sécurité à mettre en œuvre pour leur déploiement dans l'environnement du cégep. La gestion des risques liés à la sécurité de l'information s'inscrit dans le processus global de gestion des risques du cégep. Les risques à portée gouvernementale sont déclarés conformément à la Directive sur la sécurité de l'information gouvernementale.

Le niveau de protection de l'information est établi en fonction :

- de la nature de l'information et de son importance;
- des probabilités d'accident, d'erreur ou de malveillance auxquels elle est exposée;
- des conséquences de la matérialisation de ces risques;
- du niveau de risque acceptable par le cégep.

Gestion des incidents

Le cégep déploie des mesures de sécurité de l'information de manière à assurer la continuité de ses services.

À cet égard, il met en place les mesures nécessaires à l'obtention des buts suivants :

- limiter l'occurrence des incidents en matière de sécurité de l'information;

- gérer adéquatement ces incidents pour en minimiser les conséquences et rétablir les activités ou les opérations.

Les incidents de sécurité de l'information gouvernementale sont déclarés conformément à la *Directive sur la sécurité de l'information gouvernementale*. (par le CERT/AQ)

Dans la gestion des incidents, le cégep peut exercer ses pouvoirs et ses prérogatives en égard à toute utilisation inappropriée de l'information qu'il détient ou de ses systèmes d'information.

Sensibilisation et information

La sécurité de l'information repose notamment sur la régulation des conduites et à la responsabilisation individuelle. À cet égard, les membres de la communauté du cégep doivent être sensibilisés :

- à la sécurité de l'information et des systèmes d'information du cégep;
- aux conséquences d'une atteinte à la sécurité;
- à leur rôle et à leurs responsabilités en la matière.

À ces fins, des activités de sensibilisation et de formation sont offertes périodiquement. De plus, des documents explicatifs sont disponibles sur le site Internet du cégep.

Sanctions

En cas de contravention à la présente politique, l'utilisateur engage sa responsabilité personnelle; il en est de même pour la personne qui, par négligence ou par omission, fait en sorte que l'information n'est pas protégée adéquatement.

Tout membre de la communauté collégiale 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 ou des règles disciplinaires internes applicables.

De même, toute contravention à la politique, qu'elle soit perpétrée par un fournisseur, un partenaire, un invité, un consultant ou un organisme externe, est passible des sanctions prévues au contrat le liant au cégep ou en vertu des dispositions de la législation applicable en la matière.

7. RÔLES ET RESPONSABILITÉS

La présente politique attribue la gestion de la sécurité de l'information du cégep à des instances, à des comités et à des personnes en raison des fonctions particulières qu'elles exercent.

7.1 Conseil d'administration

Le conseil d'administration adopte la *Politique de sécurité de l'information* ainsi que toute modification à celle-ci. Le conseil est régulièrement informé des actions du cégep en matière de sécurité de l'information. Il est le dirigeant de l'organisme responsable de l'application de la politique en sécurité de l'information.

Le comité exécutif du conseil d'administration peut prendre des décisions dans un cadre déterminé préalablement par ce dernier.

7.2 Comité de direction

Le comité de direction du cégep détermine des mesures visant à favoriser l'application de la politique et des obligations légales du cégep en matière de sécurité de l'information. Ainsi, il détermine les orientations stratégiques, les plans d'action et les bilans de sécurité de l'information. Il peut également déterminer des directives et des procédures qui viennent préciser ou soutenir l'application de la politique.

7.3 Comité de travail pour la sécurité de l'information

Le comité de travail pour la sécurité de l'information a comme objectif d'assister le responsable de la sécurité de l'information (RSI) à mettre en place la cadre de gestion de la sécurité de l'information et autre élément pouvant être nécessaire pour assurer la protection du cégep et être conforme à la réglementation.

Ce comité est chargé en particulier de mettre en place la cadre de gestion, les plans d'action et les bilans de sécurité de l'information, les activités de sensibilisation ou de formation ainsi que toutes propositions d'action en matière de sécurité de l'information. C'est aussi un forum d'échange entre les parties prenantes ou d'observation de l'évolution du projet en sécurité de l'information.

Le comité sera formé des parties prenantes du cégep qui seront directement concernées ou qui participent au projet de mise en place de la sécurité de l'information.

7.4 Directeur général

Le directeur général veille à l'application de la politique sur la sécurité de l'information.

Cette personne aura pour tâche :

- d'encadrer le responsable de la sécurité de l'information (RSI) dans la réalisation de son mandat;
- de déléguer certaines responsabilités au secrétaire général pour la gestion de l'information;

- de faire adopter par le CA les orientations stratégiques, les évaluations de risques, les plans d'action, les bilans de sécurité, les redditions de comptes en matière de sécurité de l'information;

- d'autoriser, de façon exceptionnelle, une dérogation à l'une ou l'autre des dispositions de la présente politique, d'une directive ou d'une procédure institutionnelle ayant une incidence directe ou indirecte sur la sécurité de l'information et qui serait incompatible avec une activité ou un projet directement relié à la mission du cégep;

- d'autoriser une enquête lorsqu'il y a ou pourrait y avoir transgression de la politique;

- de ternir à jour le registre des dérogations et le registre des cas de contravention à la présente politique.

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

La fonction du RSI est déléguée à un cadre par le conseil d'administration. Le RSI relève du directeur général au sens du Cadre gouvernemental de gestion de la sécurité de l'information. Cette personne met en place le cadre de gestion de la sécurité de l'information et s'assure que le niveau de maturité en gestion de la sécurité de l'information répond aux besoins. Il est nommé par le conseil d'administration.

Le RSI :

- élabore et propose le programme de sécurité de l'information du cégep, rend compte de son implantation au comité de direction;

- formule des recommandations concernant les besoins, les priorités, les orientations, les plans d'action, les directives, les procédures, les initiatives et les bonnes pratiques en matière de sécurité de l'information et met à jour la politique;

- assure la coordination et la cohérence des actions menées au sein du cégep en matière de sécurité de l'information, en conseillant les responsables d'actifs informationnels dans les unités;

- produit les plans d'action, les bilans et les redditions de comptes du cégep en matière de sécurité de l'information;

- propose des dispositions visant le respect des exigences en matière de sécurité de l'information à intégrer dans les ententes de service et les contrats;

- s'assure de la déclaration par le cégep des risques et des incidents de sécurité de l'information à portée gouvernementale (CERT/AQ);

- collabore à l'élaboration du contenu du plan de communication, du programme de sensibilisation et de formation en matière de sécurité de l'information et veille au déploiement de ceux-ci;

- procède aux enquêtes dans des transgressions sérieuses ayant trait présumément à la politique à la suite de l'autorisation du dirigeant de l'organisme;

- s'assure des veilles normatives, juridiques, gouvernementales et technologiques afin de suivre l'évolution des normes, des lois et règlements, des pratiques gouvernementales et des progrès technologiques en matière de sécurité de l'information.

7.6 Service informatique

En matière de sécurité de l'information, l'informatique s'assure de la prise en charge des exigences de sécurité de l'information dans l'exploitation des systèmes d'information de même que dans la réalisation de projets de développement ou d'acquisition de systèmes d'information dans lesquels il intervient :

- il participe activement à l'analyse de risques, à l'évaluation des besoins et des mesures à mettre en œuvre, et à l'anticipation de toute menace en matière de sécurité des systèmes d'information faisant appel aux technologies de l'information;

- il applique des mesures de réaction appropriées à tout incident de sécurité de l'information, telles que par exemple l'interruption ou la révocation temporaire – lorsque les circonstances l'exigent – des services d'un système d'information faisant appel aux technologies de l'information, et ce, en vue d'assurer la sécurité de l'information en cause;

- il participe à l'exécution des enquêtes relatives à des contraventions réelles ou apparentes à la présente politique et autorisées par le directeur général.

7.7 Service des ressources matérielles

Le service des ressources matérielles participe, avec le responsable de la sécurité de l'information, à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du cégep.

7.8 Service des ressources humaines

En matière de sécurité de l'information, le service des ressources humaines obtient de tout nouvel employé du cégep, après lui en avoir montré la nécessité, son engagement au respect de la politique.

7.9 Responsable d'actifs informationnels

Le responsable d'actifs informationnels est le cadre détenant l'autorité au sein d'un service, qu'elle soit d'ordre pédagogique ou d'ordre administratif, et dont le rôle consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels sous la responsabilité de ce service. Il peut donc y avoir plusieurs responsables d'actifs informationnels dans un cégep. Le responsable d'actifs informationnels peut déléguer la totalité ou bien une partie de sa responsabilité à un autre membre du service.

Le responsable d'actifs informationnels :

- informe le personnel relevant de son autorité et les tiers avec lesquels transige le service de la politique de sécurité de l'information et des dispositions du cadre de gestion dans le but de le sensibiliser à la nécessité de s'y conformer;
- collabore activement à la catégorisation de l'information du service sous sa responsabilité et à l'analyse de risques;
- voit à la protection de l'information et des systèmes d'information sous sa responsabilité et veille à ce que ceux-ci soient utilisés par le personnel relevant de son autorité en conformité avec la politique de sécurité de l'information et de tout autre élément du cadre de gestion;
- s'assure que les exigences en matière de sécurité de l'information sont prises en compte dans tout processus d'acquisition et tout contrat de service sous sa responsabilité et voit à ce que tout consultant, fournisseur, partenaire, invité, organisme ou firme externe s'engage à respecter la politique et tout autre élément du cadre de gestion;
- rapporte au service informatique toute menace ou tout incident afférent à la sécurité de l'information;
- collabore à la mise en œuvre de toute mesure visant à améliorer la sécurité de l'information ou à remédier à un incident de sécurité de l'information ainsi qu'à toute opération de vérification de la sécurité de l'information;
- rapporte au directeur général tout problème lié à l'application de la présente politique, dont toute contravention réelle ou apparente d'un membre du personnel à ce qui a trait à l'application de cette politique.

7.10 Utilisateurs

La responsabilité de la sécurité de l'information du cégep incombe à tous les utilisateurs des actifs informationnels du cégep.

Tout utilisateur qui accède à une information, qui la consulte ou qui la traite est responsable de l'utilisation qu'il en fait et doit procéder de manière à protéger cette information.

À cette fin, l'utilisateur doit :

- se conformer à la présente politique et à toute autre directive du cégep en matière de sécurité de l'information et d'utilisation des actifs informationnels;
- utiliser les droits d'accès qui lui sont attribués et autorisés, l'information et les systèmes d'information qui sont mis à sa disposition uniquement dans le cadre de ses fonctions et aux fins auxquelles ils sont destinés;
- participer à la catégorisation de l'information de son service;
- respecter les mesures de sécurité mises en place, ne pas les contourner ni modifier leur configuration ni les désactiver;
- signaler au responsable des actifs informationnels de son unité tout incident susceptible de constituer une contravention à la présente politique ou de constituer une menace à la sécurité de l'information du cégep;
- collaborer à toute intervention visant à indiquer ou à mitiger une menace à la sécurité de l'information ou un incident de sécurité de l'information;

Aussi, tout utilisateur du cégep doit se conformer aux politiques et aux directives en vigueur dans une entreprise ou un organisme avec lequel il est en relation dans le cadre de ses activités professionnelles ou d'études lorsqu'il y partage des actifs informationnels, des dispositifs de technologies de l'information ou des systèmes d'information.

8. DIFFUSION ET MISE À JOUR DE LA POLITIQUE

Le RSI, assisté par le comité de travail pour la sécurité de l'information, est responsable de la diffusion et de la mise à jour de la politique. La politique de sécurité de l'information sera révisée au plus tard trois ans après son approbation.

9. APPROBATION

La présente politique entre en vigueur à la date de son adoption par le conseil d'administration, soit le 14 juin 2017.