cégep drummond

POLITIQUE N° 11

POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION

Modifiée le 29 avril 2025

960, rue Saint-Georges
Drummondville (Québec) J2C 6A2

Téléphone : 819 478-4671
Télécopieur : 819 474-6859

cegepdrummond.ca

Adoptée au conseil d'administration :
Politique de gestion des documents administratifs :
14 juin 2005 (CA-2005-06-14-19)

Politique sur la sécurité de l'information :
5 mai 2020 (CA-2020-05-05-14)
Modifiée :
29 avril 2025 (CA-2025-04-29-10)

© Cégep de Drummondville

960, rue Saint-Georges
Drummondville (Québec) J2C 6A2
www.cegepdrummond.ca

819.478.4671
info@cegepdrummond.ca

TABLE DES MATIÈRES

1. Préambule

L'entrée en vigueur de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, ainsi que de la Directive sur la sécurité de l'information gouvernementale, 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 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.

Cette politique permet au Cégep de Drummondville de s'acquitter de ses obligations légales et réglementaires. Elle permet aussi la mise en place de mécanismes servant à réduire les risques liés à la gestion de l'information qu'il a produite ou reçue. Cette information est multiple et diversifiée. Elle consiste notamment en des renseignements personnels d'étudiantes et d'étudiants et de membres du personnel, en de l'information professionnelle sujette à des droits de propriétés intellectuelles (enseignantes et enseignants, chercheuses et chercheurs) et, finalement, en de l'information stratégique ou opérationnelle pour l'administration du cégep.

2. Définitions

Actif informationnel : Tout document dont la définition correspond à celle de l'article 3 de la Loi concernant le cadre juridique des technologies de l'information (chapitre C-1.1). À titre de rappel, cette loi définit le document comme étant : « Un 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 ».

Cette même loi assimile 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.

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

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.

Confidentialité : Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées.

Cycle de vie de l'information : L'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'organisme public.

3. Cadre légal et administratif

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

- 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 et 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 modernisant des dispositions législatives en matière de protection des renseignements personnels (RLRQ, 2021, chapitre 25);
- la Loi sur les archives (LRQ, chapitre A-21.1);
- la Loi sur l'administration publique (LRQ, chapitre A-6.01);
- la Loi sur la fonction publique (LRQ, chapitre F-3.1.1);
- 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 (chapitre A-2.1, r. 02);
- la Directive sur la sécurité de l'information gouvernementale;
- la Directive sur les services de certification offerts par le gouvernement du Québec pendant la phase intérimaire.

4. Objectifs de la politique

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, quel que soit le support ou les moyens de communication utilisés. Plus spécifiquement, le Cégep doit veiller à:

- La disponibilité de l'information de façon qu'elle soit accessible en temps voulu et de la manière requise pour les personnes autorisées;

- L'intégrité de l'information de manière 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.

De plus, un Cadre de gestion de la sécurité de l'information (voir section 7) structure 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.

5. Champ d'application

La présente politique s'adresse aux utilisatrices et utilisateurs, c'est-à-dire à tout le personnel, peu importe son statut, à toute personne physique ou morale qui, à titre d'employé, de consultant, de partenaire ou de fournisseur, utilise les actifs informationnels du Cégep de Drummondville ou y a accès ainsi qu'à toute personne dûment autorisée à y avoir accès.

L'information visée est celle que le Cégep de Drummondville détient dans l'exercice de ses fonctions, que sa conservation soit assurée par lui-même ou par un tiers.

Le Collège, en tant que personne morale, est propriétaire de l'actif informationnel.

6. Énoncés de principes généraux

La Politique de sécurité de l'information demande la mise en place de mécanismes permettant de:

- Reconnaître, identifier, analyser ainsi que de mitiger les risques :
  - pouvant porter atteinte aux actifs informationnels propres et sous la gouverne du collège;
  - en regard des informations propres à la vie privée des individus, notamment, la confidentialité des renseignements à caractère nominatif de la clientèle étudiante, du personnel ou de tout partenaire d'affaires du collège;
- Assurer la gestion des accès et des actifs (disponibilité et révocabilité);
- Assurer la surveillance et l'intégrité des réseaux informatiques, des télécommunications, d'Internet et des actifs physiques et informationnels;
- Assurer le respect de la vie privée des individus, notamment, la confidentialité des renseignements à caractère nominatif relatif à la clientèle étudiante, au personnel du collège et à tout partenaire d'affaires du collège provenant du milieu des affaires ou de l'industrie ;

- Assurer la conformité aux lois et règlements applicables ;
- Définir, établir et maintenir un plan de continuité et de relève des services informatiques du collège.

7. Protection de l'information

a) Le Cégep de Drummondville 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 pratiques reconnues et généralement utilisées, tant à l'échelle nationale qu'à l'échelle internationale.

b) Le Cégep de Drummondville reconnaît que les actifs informationnels qu'il 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'accident, d'erreur et de malveillance auxquels ils sont exposés.

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

7.1 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;
- tout renseignement dont la divulgation aurait des incidences, notamment sur les relations intergouvernementales, les négociations entre organismes publics ou l'économie;
- les renseignements concernant les tiers relativement à leurs données industrielles, financières, commerciales, scientifiques ou techniques;
- l'administration de la justice et la sécurité publique;
- les décisions administratives ou politiques;
- les activités de vérification.

7.2 Sensibilisation et formation

Le Cégep de Drummondville s'engage, sur une base régulière, à sensibiliser et à former les utilisatrices et utilisateurs à la sécurité des actifs informationnels, aux conséquences d'une atteinte à leur sécurité ainsi qu'à leur rôle et leurs obligations en la matière.

7.3 Droit de regard

Le Cégep de Drummondville, par le rôle de ses officiers et par l'attribution de responsabilités à des personnes désignées, exerce, en conformité avec la législation et la réglementation en vigueur, un droit de regard sur tout usage de ses actifs informationnels. Des balises encadrent clairement les conditions d'exercice de ce droit, notamment par la tenue d'un registre par le responsable de la sécurité de l'information et par un mécanisme d'autorisation du supérieur immédiat.

7.4 Cadre de gestion de la sécurité de l'information

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 de l'information permettant notamment une reddition de comptes adéquate.

Les pratiques et les solutions retenues en matière de sécurité de l'information doivent être revues de façon périodique dans le but de tenir compte non seulement des changements juridiques, organisationnels, technologiques, physiques et environnementaux, mais aussi de l'évolution des menaces et des risques.

Le Cadre de gestion de la sécurité de l'information ainsi que les procédures mises en place au Cégep de Drummondville se trouvent dans la Politique n°29 relative à l'utilisation des technologies de l'information et des communications.

7.5 Gestion des accès

La gestion des accès doit être encadrée et contrôlée afin 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 responsabilités et une imputabilité des personnes, à tous les niveaux pour l'ensemble du personnel du cégep.

7.6 Gestion des actifs informationnels et matériels

La gestion des actifs assure l'identification de l'ensemble des systèmes d'information qui supportent la mission ainsi que les obligations légales, institutionnelles et contractuelles de l'organisation. Le processus d'inventaire est instrumental dans la catégorisation et de la classification des actifs de l'organisation (logiciels, données, systèmes et composantes de ces derniers) tout en y assurant la gestion et doit être maintenu à jour sur une base continue et contrôlée.

7.7 Gestion des risques

On appelle un risque tout événement comportant un certain degré d'incertitude et qui pourrait porter atteinte à la confidentialité, à l'intégrité ou à la disponibilité de l'information et ainsi causer un préjudice. La gestion des risques est une approche systémique permettant aux gestionnaires de prendre des décisions éclairées en contexte d'incertitude, en considérant les enjeux importants liés aux risques et à la sécurité de l'information.

Une catégorisation des actifs informationnels à jour soutient l'analyse des 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 et maintien 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. En général, 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 auxquelles elle est exposée;
- Des conséquences et de l'impact de la matérialisation de ces risques;
- Définition des niveaux de risques acceptables par le Cégep.

7.8 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'atteinte des buts suivants :

- Limiter l'occurrence des incidents en matière de sécurité de l'information;
- Gérer adéquatement ces incidents pour en minimiser les conséquences tout en permettant le rétablissement des activités et des opérations à l'intérieur d'une période acceptable.

Tout incident de sécurité de l'information doit être communiqué à la Direction générale et déclaré par le Responsable de la sécurité de l'information (RSI) conformément à la Directive sur la sécurité de l'information gouvernementale, et ce, en lien avec le CERT/AQ.

Lors de l'activation des actions encadrées par la gestion des incidents, le Cégep peut exercer ses pouvoirs et ses prérogatives en égard à toute utilisation inappropriée des actifs (informationnels et installation physique) qu'il détient ou de ses systèmes d'information (sur site ou services).

8. 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.

8.1 Conseil d'administration

Le conseil d'administration est l'autorité adoptant la Politique de sécurité de l'information ainsi que toute modification à celle-ci.

8.2 Régie de direction

La régie de direction du cégep détermine des mesures visant à favoriser l'application de cette politique et des obligations légales du cégep en matière de sécurité de l'information. À partir des bilans de sécurité, elle détermine les plans d'action, les directives et les procédures qui viennent préciser ou soutenir l'application de la politique. Au besoin, la régie de direction assiste le responsable de la sécurité de l'information (RSI) afin de mettre en place le Cadre de gestion de la sécurité de l'information et tout autre élément pouvant être nécessaires pour assurer la protection de l'actif informationnel du cégep.

8.3 Direction générale

La direction générale est responsable de l'application de la Politique de sécurité de l'information. Elle a pour tâche :

- De nommer et 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;
- D'autoriser une enquête et une supervision lorsqu'il y a ou pourrait y avoir transgression de la politique.

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

Le responsable de la sécurité de l'information est responsable, notamment de la mise en place du Cadre de gestion de la sécurité de l'information et d'assurer que le niveau de maturité, en gestion de la sécurité de l'information, répond aux besoins. Il a pour tâche de:

- Élaborer et proposer un Cadre de gestion de la sécurité de l'information;
- Rendre compte de son implantation au comité de direction;
- Formuler 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 mettre à jour la politique;
- Assurer 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;
- Produire les plans d'action, les bilans et les redditions de comptes du cégep en matière de sécurité de l'information;
- Proposer 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'assurer de la déclaration par le Cégep des risques et des incidents de sécurité de l'information à portée gouvernementale (CERT/AQ);
- À la suite de l'autorisation du directeur général, procéder aux enquêtes ou supervisions dans des cas de transgressions sérieuses;
- S'assurer 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.

8.5 Service intégré des technologies de l'information

Le Service des technologies de l'information participe, avec le responsable de la sécurité de l'information, à l'identification, à l'installation et au maintien des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du cégep. Ce service 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 de la sécurité de l'information.

8.6 Direction des ressources humaines et des affaires corporatives

En matière de sécurité de l'information, la Direction des ressources humaines obtient de tout nouveau membre du personnel du cégep, après lui en avoir montré la nécessité, son engagement au respect de la politique. Le secrétariat général est responsable de l'accès à l'information et de

la protection des renseignements personnels. Le secrétariat général travaille en étroite collaboration avec le responsable de la sécurité de l'information.

8.7 Responsable d'actifs informationnels

Le responsable des actifs informationnels est obligatoirement un gestionnaire détenant l'autorité au sein d'un service, qu'elle soit d'ordre pédagogique ou d'ordre administratif. Le responsable d'actif informationnel :

- Informe le personnel relevant de son autorité et les tiers avec lesquels transige le service de cette et des autres dispositions réglementaires 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;
- Informe le service des technologies de l'information, de toute menace ou tout incident afférant 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;
- Informe le 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.

8.8 Utilisatrices et utilisateurs

La responsabilité de la sécurité de l'information incombe à toutes les utilisatrices et tous les utilisateurs des actifs informationnels. Ainsi, toute utilisatrice et 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 diligente afin de protéger cette information. À cette fin, l'utilisatrice ou l'utilisateur :

- Se conforme à la présente politique et à toute autre directive du cégep en matière de sécurité de l'information et d'utilisation des actifs informationnels;

- Utilise uniquement 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;
- Participe à la catégorisation de l'information de son service;
- Respecte les mesures de sécurité mises en place, ne pas les contourner ni modifier leur configuration ni les désactiver;
- Signale 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;
- Collabore 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, toute utilisatrice et tout utilisateur 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.

9. Sanctions

En cas de contravention à la présente politique, l'utilisatrice ou 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 (conventions collectives de travail et du Règlement du collège). 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.

10. Dispositions finales

10.1 Entrée en vigueur

La Politique de sécurité de l'information entre en vigueur au moment de son adoption, par résolution, par le conseil d'administration.

10.2 Diffusion

La sécurité de l'information repose notamment sur la régulation des conduites et la responsabilisation individuelle. À cet égard, les membres de la communauté du cégep doivent être sensibilisés aux bonnes pratiques. À cet égard, le Cégep met en place les moyens de diffusion suivants :

- Cette politique est diffusée auprès de toute la communauté du cégep dès son entrée en vigueur;
- Des documents explicatifs sont rendus disponibles sur le site Internet du cégep;
- Des activités de sensibilisation et de formation sont offertes périodiquement et au besoin.

10.3 Révision

La Politique de sécurité de l'information doit être révisée au besoin et au minimum une fois tous les cinq (5) ans à compter de son adoption. La révision est déclenchée par la direction générale en appliquant la procédure suivante :

- Le RSI effectue les travaux de vigie technologique et organisationnelle, permettant de proposer les révisions applicables au contexte de l'organisation;
- Propose et présente les amendements intégrés au document révisé à la régie de direction pour examen et, le cas échéant, modifications;
- La régie de direction recommande au conseil d'administration l'adoption de la politique.