Directive sur la gestion des incidents de confidentialité

1. Préambule

La présente Directive découle de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (ci-après- « Loi sur l'accès ») et de la *Politique sur la protection des renseignements personnels* du Cégep. Le contenu du présent document est grandement inspiré du *Règlement sur les incidents de confidentialité* adopté par le gouvernement du Québec par le Décret 1761-2022 le 30 novembre 2022, du *Guide de rédaction des règles de gouvernance en matière de protection des renseignements personnels* (2023) de la Direction des affaires juridiques de la Fédération des cégeps et des éléments recommandés par la Commission sur l'accès à l'information sur son site web. La Directive a été approuvée par le Comité sur l'accès à l'information et la protection des renseignements personnels le 1er juin 2023 et par le Comité de direction du Cégep le 6 juin 2023.

Tel que le prévoit la *Politique sur la protection des renseignements personnels*, le Cégep reconnait l'importance de protéger les renseignements personnels qu'il détient. Afin de s'acquitter de ses obligations en la matière, le Cégep met en place des mesures de sécurité raisonnables pour protéger les renseignements personnels qu'il traite peu importe leur support, et ce, tout au long de leur cycle de vie. Malgré les précautions prises, un incident est toujours possible. C'est pourquoi le Cégep se dote de la présente Directive pour gérer les éventuels incidents de confidentialité et limiter ainsi leurs conséquences potentielles pour les personnes concernées et le Cégep.

Les définitions prévues à la *Politique sur la protection des renseignements personnels* du Cégep et les rôles et responsabilités de la Personne responsable de l'accès aux documents et de la protection des renseignements personnels s'appliquent à la présente Directive.

2. Objectifs

La présente Directive :

- Précise ce qu'est un incident de confidentialité et décrit les étapes à suivre en cas d'incident de confidentialité;
- Rappelle l'obligation de signaler les incidents de confidentialité et indique la marche à suivre à ce niveau;
- Clarifie les rôles de la Personne responsable de l'accès aux documents et de la protection des renseignements personnels et de la Direction des systèmes et technologies de l'information (DiSTI) pour la gestion des incidents de confidentialité.

3. Définition et exemples d'incidents de confidentialité

Un incident de confidentialité correspond à tout accès, utilisation ou communication non autorisés par la loi d'un renseignement personnel, de même qu'à la perte d'un renseignement personnel ou à toute autre atteinte à sa protection. L'incident peut survenir à différentes étapes du cycle de vie de l'information, que ce soit la collecte, l'utilisation, la communication, la conservation ou la destruction du renseignement personnel. Il peut être intentionnel ou non.

Voici quelques exemples d'incidents de confidentialité :

- Le fait, pour le Cégep, d'être victime d'un hameçonnage ou d'un rançongiciel et que des renseignements personnels soient volés;
- Un pirate informatique qui s'infiltre dans un système;

- Le fait de perdre ou de se faire voler un ordinateur portable ou une tablette du Cégep ou tout autre support amovible non chiffré qui contient des renseignements personnels[1];
- Un membre du personnel qui consulte une base de données (telle que CLARA) dans le cadre de son travail, télécharge une copie de certains dossiers d'employés et se les envoie sur son adresse courriel personnel;
- Le fait de modifier des données dans une base de données en vue de défavoriser ou de favoriser une personne;
- Le fait de consulter le dossier d'une personne, sans que ce soit nécessaire dans le cadre de son travail et sans autorisation, quel que soit le support (numérique, papier);
- Le fait d'envoyer une communication (courriel, courrier ou autre) contentant des renseignements personnels au mauvais destinataire.

Il est important de distinguer un événement de sécurité de l'information (ou de cybersécurité) d'un incident de confidentialité, car chacun de ces événements entraîne des obligations distinctes. Un événement de sécurité de l'information correspond à « toute forme d'atteinte, présente ou appréhendée, telle une cyberattaque ou une menace à la confidentialité, à l'intégrité et à la disponibilité d'une information ou d'une ressource informationnelle[2] » sous la responsabilité du Cégep ou d'une personne agissant pour ce dernier.

Un événement de sécurité de l'information peut avoir lieu même en l'absence de renseignements personnels, car la définition vise toute information ou ressource informationnelle sous la responsabilité du Cégep. Un événement de sécurité couvre les atteintes présentes et appréhendées, alors qu'un incident de confidentialité concerne seulement les atteintes présentes. Ainsi, tout événement de sécurité n'est pas nécessairement un incident de confidentialité. Cependant, celui-ci constitue généralement un événement de sécurité, car il s'agit d'une atteinte à la confidentialité d'une ressource informationnelle qui, dans certains cas, peut affecter la disponibilité ou l'intégrité.

4. Procédure à suivre en cas d'incident de confidentialité

En cas d'incident de confidentialité, le Cégep suit un processus permettant une gestion efficace de l'incident rapporté.

4.1 Signalement d'un incident de confidentialité

Pour que l'événement soit un incident de confidentialité, il faut que les informations qui font l'objet de l'incident constituent des renseignements personnels confidentiels. Un événement qui aurait un impact sur des informations confidentielles peut être grave, mais ne déclenche pas les obligations de la présente Directive s'il n'implique pas de renseignements personnels.

La Politique prévoit l'obligation, pour toutes les personnes qui traitent des renseignements personnels détenus par le Cégep, de signaler à la Personne responsable de l'accès aux documents et de la protection des renseignements personnels, ou à une personne répondante en matière de protection des renseignements personnels, tout incident de confidentialité ou toute situation pouvant porter atteinte aux renseignements personnels.

Pour se faire, les membres du personnel doivent remplir le formulaire numérique disponible sur le site web du Cégep.

4.2 Évaluation de la situation et des mesures pour diminuer les risques et éviter de nouveaux incidents

Lorsque le Cégep a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'il détient, il doit, dans les meilleurs délais, prendre les mesures raisonnables pour diminuer les risques qu'un préjudice, qu'il soit sérieux ou non, soit causé et éviter que de nouveaux incidents de même nature ne se produisent.

Pour y arriver, la Personne responsable de l'accès aux documents et de la protection des renseignements personnels doit en premier lieu évaluer la situation. Les informations qui lui sont communiquées par le formulaire de signalement

---

[1] *Les membres du personnel ne devraient pas utiliser des clés USB pour y stocker des renseignements personnels; il ne s'agit pas d'une bonne pratique en matière de protection des renseignements personnels.*

[2] Comme défini dans la *Directive gouvernementale sur la sécurité de l'information* et *dans le Règlement sur les modalités et conditions d'application des articles 12.2 à 12.4 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*.

lui permettent de débuter cette évaluation. Au besoin, elle recueille toutes autres informations nécessaires à cette évaluation, en collaboration avec la personne qui a signalé l'incident, avec la personne répondante du secteur concerné et/ou avec les gestionnaires de la direction, du service ou du département concerné. Les questions suivantes sont utiles afin d'évaluer rapidement la situation :

- QUI : quelles sont les personnes concernées par l'incident et pouvant être affectées par cet incident? S'agit-il de membres du personnel, de membres de la population étudiante, d'usagères et d'usagers des services ou de partenaires d'affaires? Qui peut avoir eu accès aux renseignements personnels?
- COMBIEN : combien de personnes sont touchées par l'incident?
- QUOI : Déterminer la nature et le niveau de sensibilité des renseignements personnels impliqués, ainsi que les risques pour les personnes concernées.
- QUAND : Tenter de déterminer le plus précisément possible le moment de l'incident, ainsi que le moment de sa découverte. Un grand écart entre ces deux moments pourrait possiblement aggraver l'incident.
- OÙ : Déterminer le lieu de l'incident. Si l'incident s'est produit au Cégep, dans quel secteur? L'incident a-t-il eu lieu chez un tiers détenant des renseignements personnels pour le compte du Cégep (ex. : un mandataire, un fournisseur)?
- POURQUOI : Identifier les causes et l'origine de l'incident de confidentialité : le problème, l'erreur, la vulnérabilité, etc. Quelles mesures de sécurité étaient en place au moment de l'incident? Pourquoi n'ont-elles pas été efficaces?

Les mesures raisonnables à mettre en place dépendent de cette évaluation de la situation et peuvent prendre plusieurs formes, par exemple : faire cesser la pratique non autorisée, récupérer ou exiger la destruction des renseignements personnels impliqués, corriger les lacunes informatiques, etc. Toutes les situations sont différentes. Même si l'ensemble des informations pertinentes ne sont pas connues dès le départ, il est important que la Personne responsable de l'accès aux documents et de la protection des renseignements personnels réagisse rapidement. Au besoin, le Cégep continue d'adapter ses mesures ou à d'en adopter de nouvelles au fur et à mesure que les circonstances et les impacts de l'incident se précisent par la suite.

4.3 Évaluation des risques de préjudice sérieux

Pour tout incident de confidentialité, le Cégep doit évaluer la gravité du risque de préjudice pour les personnes visées par l'incident. Pour procéder à cette évaluation, la Personne responsable de l'accès aux documents et de la protection des renseignements personnels doit notamment considérer :

- La sensibilité des renseignements personnels concernés;
- Les conséquences appréhendées de leur utilisation (comme un vol d'identité, une fraude financière, une atteinte importante à la vie privée);
- La probabilité que ces renseignements puissent être utilisés à des fins préjudiciables.

La Personne responsable de l'accès aux documents et de la protection des renseignements personnels peut impliquer d'autres intervenants au besoin, tels que la personne responsable de la sécurité de l'information, l'analyste en gestion de l'information ou des consultants externes.

Si l'analyse fait ressortir un risque de préjudice sérieux, la Personne responsable de l'accès aux documents et de la protection des renseignements personnels devra aviser la Commission de l'accès à l'information (ci-après la « CAI ») ainsi que les personnes concernées de l'incident de confidentialité.

Si l'incident de confidentialité ne comporte aucun risque de préjudice sérieux, le Cégep, par le biais de la Personne responsable de l'accès aux documents et de la protection des renseignements personnels, doit tout de même poursuivre ses travaux pour réduire les risques et éviter qu'un incident de même nature se produise à nouveau dans le futur.

Lorsqu'un incident de confidentialité constitue également un événement de sécurité de l'information ou de cybersécurité, la Personne responsable de l'accès aux documents et de la protection des renseignements personnels avise la Personne responsable de la sécurité de l'information du Cégep et travaille de concert avec celle-ci et la Direction des systèmes et technologies de l'information (DiSTI) pour améliorer les pratiques et éviter les incidents de même nature le futur.

Lorsqu'un incident concerne un système d'information ou qu'il se produit dans le cadre de la perte, du vol ou de la disparition de matériel ou de documents, il est possible que le signalement soit fait à la DiSTI ou au Service de sécurité plutôt que par le biais du formulaire de signalement d'un incident de confidentialité. Si cela se produit, les intervenants doivent communiquer l'incident à la Personne responsable de l'accès aux documents et de la protection des renseignements personnels dans les meilleurs délais. Selon les circonstances, ces intervenants pourront être impliqués dans la gestion des incidents de confidentialité.

4.4 Avis à la CAI et aux personnes concernées

Le Cégep, par le biais de la Personne responsable de l'accès aux documents et de la protection des renseignements personnels, doit rapidement aviser la CAI dans le cas où l'incident comporte un risque de préjudice sérieux à une ou à des personnes concernées. Ces personnes doivent être également avisées par le Cégep; autrement, la CAI pourrait lui ordonner de le faire. Toutefois, le Cégep à n'a pas à aviser les personnes dont les renseignements personnels sont concernés si cela peut nuire à une enquête en vertu de la loi afin de prévenir, détecter, réprimer le crime ou les infractions aux lois.

La CAI est avisée par la transmission du modèle de formulaire fourni par celle-ci, dûment rempli, dont une copie est disponible comme Annexe 1 de la présente directive. Toute nouvelle information obtenue par la suite, doit être également acheminée le plus rapidement possible. La Commission peut demander au Cégep d'autres informations liées à l'incident de confidentialité, mais non requises par le *Règlement sur les incidents de confidentialité* (adopté par le Décret 1761-2022 le 30 novembre 2022).

L'avis à la personne concernée doit l'informer de la portée et des conséquences de l'incident présentant le risque de préjudice sérieux. Cet avis doit contenir :

- Une description des renseignements personnels visés par l'incident. Si cette information n'est pas connue, le Cégep doit communiquer la raison justifiant l'impossibilité de fournir cette description;
- Une brève description des circonstances de l'incident;
- La date ou la période où l'incident a eu lieu, ou une approximation de cette période si elle n'est pas connue;
- Une brève description des mesures prises ou envisagées pour diminuer les risques qu'un préjudice soit causé à la suite de l'incident;
- Les mesures proposées à la personne concernée afin de diminuer le risque qu'un préjudice lui soit causé ou d'atténuer celui-ci;
- Les coordonnées d'une personne ou d'un service avec qui la personne concernée peut communiquer pour obtenir davantage d'informations au sujet de l'incident.

Le Cégep peut également diffuser un avis public afin d'agir rapidement pour diminuer le risque qu'un préjudice sérieux soit causé ou pour l'atténuer. Le Cégep demeure toutefois tenu de transmettre un avis à la personne concernée dans les plus brefs délais. Seulement trois situations permettent de faire un avis public sans transmettre un avis à la personne concernée :

- La transmission de l'avis peut causer un plus grand préjudice à la personne concernée;
- La transmission de l'avis représente une difficulté excessive pour le Cégep;
- Le Cégep n'a pas les coordonnées de la personne concernée.

Cet avis peut être fait par tout moyen raisonnable permettant de joindre la personne concernée.

4.5 Avis aux personnes pouvant prévenir ou diminuer le risque de préjudice sérieux

Le Cégep peut aviser toute personne ou organisme susceptible de diminuer le risque de préjudice sérieux. Seuls les renseignements personnels nécessaires peuvent alors être communiqués sans le consentement de la personne concernée. La Personne responsable de l'accès aux documents et de la protection des renseignements personnels de l'organisation doit enregistrer cette communication dans les registres de communication des renseignements personnel prévus par la Loi sur l'accès.

4.6 Maintien du registre des incidents de confidentialité

La Personne responsable de l'accès aux documents et de la protection des renseignements personnels tient un registre dans lequel tous les incidents de confidentialité impliquant des renseignements personnels sont consignés. Autant les incidents à risque de préjudice sérieux que ceux qui ne le sont pas doivent être consignés au registre. À la demande de la CAI, le Cégep doit lui fournir copie de son registre. Ce dernier doit contenir les informations suivantes :

- Le numéro interne de l'incident;
- Une description des renseignements personnels visés par l'incident. Si cette information est inconnue, le Cégep devra justifier pourquoi il n'est pas en mesure de fournir cette information;
- Une brève description des circonstances de l'incident;
- La date ou la période où l'incident a eu lieu, ou une approximation de cette période si elle n'est pas connue;
- La date ou la période au cours de laquelle le Cégep a pris connaissance de l'incident;
- Le nombre de personne affectées par l'incident ou, s'il n'est pas connu, une approximation de ce nombre;
- La description des éléments sur lesquels le Cégep se base pour conclure qu'il existe ou non un risque qu'un préjudice sérieux soit causé aux personnes concernées, tels que :
    - La sensibilité des renseignements personnels concernées;
    - Les utilisations malveillantes possibles des renseignements;
    - Les conséquences appréhendées de l'utilisation des renseignements et de la probabilité qu'ils soient utilisés à des fins préjudiciables.
- Les dates de transmission des avis à CAI et aux personnes concernées lorsque l'incident présente un risque de préjudice sérieux. Il faut également indiquer si le Cégep a émis des avis publics et, le cas échéant, expliquer la raison de ceux-ci;
- Une brève description des mesures prises par le Cégep à la suite de l'incident pour diminuer les risques qu'un préjudice soit causé.

Le contenu du registre est mis à jour et conservé pour une période de sept (7) ans après la date ou la période de prise de connaissance de l'incident.

5. Pouvoir d'ordonnance de la Commission

La CAI peut ordonner à toute personne, une fois que celle-ci a présenté ses observations, l'application de mesures en vue de protéger les droits des personnes concernées. Elle peut également ordonner la remise des renseignements personnels impliqués au Cégep ou leur destruction.

Dans le cas d'un incident portant un risque de préjudice sérieux, la CAI peut ordonner au Cégep d'aviser les personnes affectées si cela n'avait pas été fait.

6. Responsabilité des renseignements personnels conservés par un tiers

Le Cégep est responsable des renseignements personnels confiés à des tiers pour leur conservation. Les mesures citées dans cette directive s'appliquent donc dans ce cas.

7. Conservation des documents

La Direction du développement institutionnel et secrétariat général est responsable de la conservation des documents générés en application de la présente Directive, conformément aux délais prévus dans le calendrier de conservation du Cégep.