

PROC-21 Procédure de traitement d'un incident de confidentialité

Adoptée par l'Équipe de direction générale le 27 février 2024

TABLE DES MATIÈRES

PRÉAMBULE	3
ARTICLE 1. CHAMP D'APPLICATION.....	3
ARTICLE 2. CADRE DE RÉFÉRENCE.....	3
ARTICLE 3. DÉFINITIONS.....	3
ARTICLE 4. SIGNALEMENT D'UN INCIDENT DE CONFIDENTIALITÉ	4
ARTICLE 5. ÉVALUATION DE L'INCIDENT DE CONFIDENTIALITÉ.....	4
ARTICLE 6. RISQUE DE PRÉJUDICE SÉRIEUX	5
ARTICLE 7. ACTIONS À LA SUITE DE L'INCIDENT DE CONFIDENTIALITÉ	5
7.1. Mesures correctrices	5
7.2. Personnes à prévenir.....	5
7.3. Avis public	6
ARTICLE 8. RÔLES ET RESPONSABILITÉS	6
8.1. Membre de la communauté collégiale	6
8.2. Responsable de la protection des renseignements personnels	6
8.3. CAIPRP	7
8.4. Direction des communications et des relations publiques (DCOMRP)	7
8.5. Direction des technologies informatiques (DTI).....	7
8.6. Secteur de la gestion documentaire (GD).....	8
ARTICLE 9. REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ	8
9.1. Contenu du registre des incidents de confidentialité	8
9.2. Conservation et destruction du registre	9
ARTICLE 10. RESPONSABLE DE L'APPLICATION	9
ARTICLE 11. RESPONSABLE DE LA DIFFUSION.....	9
ARTICLE 12. ENTRÉE EN VIGUEUR.....	9
ARTICLE 13. RÉVISION	9
ANNEXE 1. REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ	10

PRÉAMBULE

Le Cégep Garneau (« le Cégep ») est responsable de la protection des renseignements personnels qu'il détient, de leur collecte à la fin de leur cycle de vie et, notamment de la conservation sécurisée ou la destruction.

Conformément à l'article 63.7 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (la *Loi sur l'accès*), lorsque le Cégep a des motifs de croire qu'un incident de confidentialité impliquant des renseignements personnels qu'il détient s'est produit, il doit prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent.

En ce sens, et afin d'assurer la transparence de ses actions en tant qu'organisme public, le Cégep se dote de la présente *Procédure de traitement d'un incident de confidentialité* (*Procédure 21*), uniformisant les pratiques dans la gestion desdits incidents.

ARTICLE 1. CHAMP D'APPLICATION

La présente *Procédure 21* s'applique à tout incident de confidentialité impliquant des renseignements personnels détenus par le Cégep, réel ou présumé, détecté par un ou une membre de la communauté collégiale.

La présente *Procédure 21* s'applique à toute personne liée ou ayant été liée au Cégep en tant que membre de la communauté collégiale et s'étend également aux tiers auxquels le Cégep communique des renseignements personnels, tous fournisseurs ou partenaires du Cégep, incluant les sous-traitants.

ARTICLE 2. CADRE DE RÉFÉRENCE

La présente *Procédure 21* est instituée en tenant compte, notamment, du cadre de référence suivant :

- la *Loi sur l'accès aux documents des organismes publics et sur la protection des Renseignements personnels*, RLRQ c. A-2.1 et ses règlements ;
- le *Règlement sur la protection des renseignements personnels* (R-07) ;
- la *Politique sur la sécurité de l'information* (POL-15) ;
- la *Politique de confidentialité*.

ARTICLE 3. DÉFINITIONS

Dans la présente *Procédure 21*, à moins que le contexte ne s'y oppose, les mots suivants sont définis comme suit :

- a) comité (CAIPRP) :** le Comité sur l'accès à l'information et la protection des renseignements personnels (CAIPRP) dont le mandat est institué par la *Directive relative au mandat du Comité de l'accès à l'information et de la protection des renseignements personnels* (DIR-10) (CAIPRP).
- b) communauté collégiale :** toute personne qui travaille, étudie ou qui a un lien avec le Cégep.

Y sont inclus notamment : toutes les personnes employées, les cadres, les étudiantes et étudiants, les stagiaires, les membres du Conseil d'administration, la clientèle des différents services, les bénévoles, les personnes sous-traitantes, les fournisseuses et fournisseurs, les partenaires, les accompagnatrices et accompagnateurs, les visiteuses et visiteurs et le personnel des corporations affiliées au Cégep dont les syndicats, l'Association générale étudiante, l'Association des parents et la Fondation.

c) incident de confidentialité : tout atteinte à la protection d'un renseignement personnel, comme prévu à l'article 63.9 de la *Loi sur l'accès*.

d) incident majeur : tout incident de confidentialité qui, lors de son évaluation préliminaire, laisse croire qu'il est susceptible de causer un préjudice sérieux aux personnes concernées, notamment en raison de la sensibilité des renseignements, des conséquences appréhendées de leur utilisation et de la probabilité qu'ils soient utilisés à des fins préjudiciables.

Toute perte ou tout vol de document ou de support technologique contenant des renseignements personnels est présumé être un incident majeur.

e) personne concernée : personne dont les renseignements personnels sont exposés à un risque en raison de la survenance de l'incident de confidentialité.

f) renseignement personnel : tout renseignement qui concerne une personne physique et qui permet directement ou indirectement de l'identifier, comme prévu à l'article 54 de la *Loi sur l'accès*.

Y sont notamment inclus : le nom, l'adresse, le numéro de téléphone, l'adresse courriel, l'occupation, le numéro d'assurance sociale, la date de naissance, la photographie et les coordonnées bancaires.

Les renseignements personnels doivent être protégés, peu importe la nature de leur support, et quelle que soit leur forme : écrite, graphique, sonore, visuelle, informatisée ou autre.

ARTICLE 4. SIGNALEMENT D'UN INCIDENT DE CONFIDENTIALITÉ

Toute personne membre de la communauté collégiale, tiers auxquels le Cégep communique des renseignements personnels, fournisseurs ou partenaires du Cégep, incluant les sous-traitants, doit effectuer un signalement lorsqu'il a un motif raisonnable de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel détenu par le Cégep.

Les incidents de confidentialité doivent être signalés à la personne responsable de la protection des renseignements personnels dans un délai de vingt-quatre (24) heures ouvrables après la connaissance dudit incident.

En dehors des heures normales de bureau, et en cas d'urgence nécessitant de prendre les actions raisonnables pour limiter l'étendue de la pratique non autorisée et l'arrêter, tout membre de la communauté collégiale doit rapporter l'incident de confidentialité à la sécurité du Cégep et à la Direction des technologies informatiques (DTI), lesquelles aviseront la personne responsable de la protection des renseignements personnels.

Tout incident de confidentialité doit être signalé, et ce, même si les circonstances laissent croire qu'il ne s'agit pas d'un incident réel ou qu'il ne causera aucun préjudice aux personnes concernées.

ARTICLE 5. ÉVALUATION DE L'INCIDENT DE CONFIDENTIALITÉ

La personne responsable de la protection des renseignements personnels détermine si la situation signalée correspond à un incident de confidentialité et entreprend les mesures appropriées.

La personne responsable de la protection des renseignements personnels évalue :

- la sensibilité des renseignements personnels visés ;
- les conséquences appréhendées de l'utilisation des renseignements personnels ;
- la probabilité que ces renseignements personnels puissent être utilisés à des fins préjudiciables.

Dès lors qu'elle a procédé à ladite évaluation, la personne responsable de la protection des renseignements personnels détermine son seuil de gravité et le traitement de l'incident.

ARTICLE 6. RISQUE DE PRÉJUDICE SÉRIEUX

Lorsque la personne responsable de la protection des renseignements personnels estime que l'atteinte à la protection desdits renseignements personnels constitue un incident majeur et donc, qu'il présente un risque de préjudice sérieux, elle coordonne, au besoin, une réunion d'urgence avec la sécurité du Cégep, la Direction des technologies informatiques (DTI), la Direction des communications et des relations publiques (DCOMRP) ainsi que toute unité administrative dont les ressources sont jugées utiles en fonction de la nature et de la portée de l'incident de confidentialité.

Les directions concernées doivent se réunir et prendre les mesures nécessaires afin de déterminer les causes et les circonstances de l'événement et d'évaluer les risques et les impacts pour les personnes concernées au plus tard vingt-quatre (24) heures ouvrables après le signalement.

La personne responsable de la protection des renseignements personnels doit informer le CAIPRP de tout incident dont elle estime qu'il cause un risque de préjudice sérieux, sauf s'il existe un enjeu de confidentialité.

ARTICLE 7. ACTIONS À LA SUITE DE L'INCIDENT DE CONFIDENTIALITÉ

7.1. Mesures correctrices

En collaboration avec les directions concernées par l'incident de confidentialité et/ou, susceptibles d'apporter une expertise utile, la personne responsable de la protection des renseignements personnels prend les mesures nécessaires afin de/d' :

- comprendre la nature de l'incident ;
- identifier les renseignements qui ont été compromis ;
- identifier et mettre en place les mesures préventives et correctrices nécessaires, c'est-à-dire étudier et adapter les documents institutionnels du Cégep, pratiques internes, formations, stratégies, mesures de sécurité ainsi que les relations d'affaires afin d'identifier les mesures qui devront être mises en place pour minimiser les effets de l'incident, corriger toutes les lacunes identifiées et réduire les risques de récurrence.

Pour mettre en place ces mesures correctrices, la personne responsable de la protection des renseignements personnels s'adjoint toute personne dont l'expertise est nécessaire.

7.2. Personnes à prévenir

Lorsqu'il a été évalué que l'incident présente un risque de préjudice sérieux et selon l'urgence de la situation, la personne responsable de l'accès à l'information et de la protection des renseignements personnels ou le CAIPRP, doit en aviser :

- la Commission d'Accès à l'Information (CAI) ;
- les personnes dont les renseignements personnels sont concernés, sauf lorsque cela serait susceptible d'entraver une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois ;
- toute personne ou toute organisation susceptible de faire cesser ou de diminuer le risque en ne lui communiquant que les renseignements personnels nécessaires, sans le consentement de la personne concernée et en enregistrant ladite communication au registre prévu au Règlement 07 ;
- les personnes responsables des contacts avec l'assureur du Cégep, le cas échéant ;
- la police, en cas de danger imminent pour la sécurité ou l'intégrité des membres de la communauté collégiale.

7.3. Avis public

Le Cégep peut donner un avis public de l'incident de confidentialité, afin d'agir rapidement pour faire cesser ou diminuer le préjudice, dans les seuls cas mentionnés ci-bas :

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

Dans ces cas, la personne responsable de la protection des renseignements personnels doit, dans les meilleurs délais et par tous les moyens raisonnables, transmettre un avis à la personne concernée.

ARTICLE 8. RÔLES ET RESPONSABILITÉS

8.1. Membre de la communauté collégiale

Toute personne qui suspecte la présence, réelle ou présumée, d'un incident de confidentialité impliquant un renseignement personnel détenu par le Cégep, ou qui a connaissance d'un tel incident doit :

- en aviser la personne responsable de la protection des renseignements personnels, ou la sécurité du Cégep, le cas échéant ;
- effectuer les actions nécessaires pour limiter l'étendue de l'incident de confidentialité, sous réserve de sa capacité et de son autorité à agir.

8.2. Responsable de la protection des renseignements personnels

En cas d'incident de confidentialité, la personne responsable de la protection des renseignements personnels prend en charge le traitement de l'incident et s'associe avec toute personne membre du personnel, capable d'apporter une expertise à la situation, notamment la Direction des technologies informatiques (DTI), le secteur de la gestion documentaire ou la sécurité du Cégep.

La personne responsable de la protection des renseignements personnels a la responsabilité de/d' :

- constater l'existence d'un incident de confidentialité et procéder à l'évaluation de sa gravité conformément à l'article 5 de la présente *Procédure* 21 ;
- aviser les personnes dont les renseignements personnels sont concernés par l'incident conformément à l'article 7.2 de la présente *Procédure* 21 ;
- aviser le chef ou à la cheffe de la sécurité de l'information organisationnelle (CSIO), conformément à l'article 7.7 de la *Politique sur la sécurité de l'information* (POL-15) ;
- aviser les personnes en contact avec les assureurs du Cégep, le cas échéant ;
- tenir le registre des incidents de confidentialité et le transmettre à la CAI, le cas échéant ;
- effectuer toute autre action lui étant déléguée par le CAIPRP.

8.3. CAIPRP

En matière d'incident de confidentialité, le CAIPRP a pour principale responsabilité :

- d'aviser la CAI, dès lors que ledit incident de confidentialité présente un risque de préjudice sérieux en utilisant le formulaire disponible en ligne.

Le CAIPRP peut déléguer la rédaction et la transmission dudit formulaire à la personne responsable de la protection des renseignements personnels.

8.4. Direction des communications et des relations publiques (DCOMRP)

En matière d'incident de confidentialité, la DCOMRP a pour responsabilité :

- de coordonner la publication de l'avis public, le cas échéant ;
- de prendre en charge les communications publiques en cas d'incident de confidentialité pouvant porter atteinte à la réputation du Cégep.

8.5. Direction des technologies informatiques (DTI)

En matière d'incident de confidentialité, la DTI est responsable de la sécurité du réseau informatique du Cégep et 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. Elle a donc la responsabilité de prendre toutes les mesures informatiques nécessaires aux fins de faire cesser ou de diminuer les risques causés par un incident de confidentialité.

La DTI évalue la situation et prend les mesures appropriées permettant de diminuer les impacts découlant de la survenance d'un incident de confidentialité sur le déroulement des activités normales du Cégep.

8.6. Secteur de la gestion documentaire (GD)

Le secteur de la GD, rattaché à la Direction des ressources humaines et des affaires corporatives (DRHAC) est responsable de la conservation et de la destruction du registre des incidents de confidentialité, conformément au *Calendrier de conservation*.

Le secteur de la GD peut également être sollicité afin de former la communauté collégiale à des pratiques saines et sécurisées en matière de gestion documentaire tant analogique que numérique, pour éviter toute reproduction d'incident de confidentialité.

ARTICLE 9. REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

9.1. Contenu du registre des incidents de confidentialité

Le Cégep doit tenir un registre dans lequel il collige tous les incidents de confidentialité impliquant des renseignements personnels, que ceux-ci présentent ou non un risque de préjudice sérieux.

À la demande de la CAI, le Cégep lui transmet une copie de son registre.

Le registre des incidents de confidentialité doit contenir les éléments suivants :

- une description des renseignements personnels visés par l'incident, ou, si cette information n'est pas connue, une 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 ;
- la date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident ;
- le nombre de personnes concernées par l'incident ou, s'il n'est pas connu, une approximation de ce nombre ;
- une description des éléments qui amènent l'organisation à conclure qu'il y a, ou non risque qu'un préjudice sérieux soit causé aux personnes concernées, comme :
 - la sensibilité des renseignements personnels concernés ;
 - les utilisations malveillantes possibles des renseignements ;
 - les conséquences appréhendées de l'utilisation des renseignements et la probabilité qu'ils soient utilisés à des fins préjudiciables ;
- les dates de transmission des avis à la CAI et aux personnes concernées, quand l'incident présente le risque de préjudice sérieux, en indiquant si des avis publics ont été donnés et la raison de ceux-ci ;
- une brève description des mesures prises par l'organisation à la suite de l'incident, pour diminuer les risques qu'un préjudice soit causé.

Un gabarit de registre est disponible à l'**Annexe 1** de la présente *Procédure 21*.

9.2. Conservation et destruction du registre

Les renseignements du registre doivent être mis à jour et conservés pour une période minimale de cinq (5) ans, après la date ou la période de prise de connaissance de l'incident par le Cégep.

La destruction sécurisée du registre est assurée par le secteur de la gestion documentaire et des archives, conformément au *Calendrier de conservation*.

ARTICLE 10. RESPONSABLE DE L'APPLICATION

La personne responsable de la protection des renseignements personnels est responsable de l'application de la présente *Procédure 21*.

ARTICLE 11. RESPONSABLE DE LA DIFFUSION

La DCOMRP est responsable de la publication et de la diffusion de la présente *Procédure 21*.

ARTICLE 12. ENTRÉE EN VIGUEUR

La présente *Procédure 21* entre en vigueur le jour de son adoption par l'Équipe de direction générale.

ARTICLE 13. RÉVISION

La présente *Procédure 21* est mise à jour lorsque l'évolution des cadres sociaux, administratifs, normatifs et juridiques le commande et minimalement tous les cinq (5) ans.

ANNEXE 1. REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

Description des circonstances de l'incident	Date ou période de l'incident (AAAA-MM-JJ)	Prise de connaissance de l'incident (AAAA-MM-JJ)	Nombre de personnes concernées par l'incident	Description des éléments qui amènent à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées	Date de transmission de l'avis à la Commission d'accès à l'information (AAAA-MM-JJ)	Date de transmission des avis aux personnes concernées (AAAA-MM-JJ)	Description des mesures prises afin de diminuer les risques qu'un préjudice soit causé