COLLÈGE DE
BOIS-DE-BOULOGNE

PROCÉDURE DE TRAITEMENT DES INCIDENTS DE CONFIDENTIALITÉ

Responsable de l'accès à l'information et de la protection des renseignements personnels
Gouvernance et affaires juridiques

Entrée en vigueur le 22 septembre 2022
Mis à jour suite à la publication du *Règlement sur les incidents de confidentialité* à la Gazette officielle du Québec (publication G.O., 14 décembre 2022, 154e année, no50, entrée en vigueur le 29 décembre 2022)

TABLE DES MATIÈRES

PRÉAMBULE

L'entrée en vigueur le 22 septembre 2022 de modifications à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignement personnels* (Loi sur l'accès) témoigne de la volonté du gouvernement de mieux protéger les renseignements personnels et de responsabiliser davantage les organismes publics. Cela permettra aux Québécoises et aux Québécois de reprendre le contrôle de leurs renseignements personnels.

En cas d'incident de confidentialité, il est exigé que les organisations prennent les mesures requises afin de réduire les risques de préjudice pour les personnes concernées et d'éviter que cela ne se reproduise.

1. OBJECTIFS

Malgré les moyens administratifs et technologiques prévus par le Collège pour que le traitement des renseignements confidentiels se fasse conformément aux lois applicables, le risque d'incident de confidentialité ne peut être complètement éliminé. Aucune mesure de prévention ou de sécurité ne peut assurer qu'aucune erreur humaine, bris technologique, perte, fraude ou cyberattaque ne survienne.

La présente procédure a pour objectif principal de guider le Collège dans le traitement d'un incident de confidentialité impliquant un renseignement personnel afin que celui-ci puisse agir efficacement et conformément aux dispositions de la Loi sur l'accès. Elle a pour but de limiter les conséquences préjudiciables pour les personnes concernées et d'éviter que la situation ne survienne de nouveau.

2. DÉFINITIONS

2.1. Incident de confidentialité : un accès non autorisé à un renseignement personnel, une utilisation ou une communication non autorisée d'un renseignement personnel, la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement. Exemples :

- 2.1.1. Un membre du personnel qui consulte des renseignements personnels non nécessaires à l'exercice de ses fonctions en outrepassant les droits d'accès qui lui ont été consentis, ou un pirate informatique qui s'infiltre dans un système;
- 2.1.2. Un membre du personnel qui utilise des renseignements personnels d'une base de données à laquelle il a accès dans le cadre de ses fonctions dans le but d'usurper l'identité d'une personne;
- 2.1.3. Une communication contenant des renseignements personnels faite par erreur à la mauvaise personne par son employeur;
- 2.1.4. Une personne qui perd ou se fait voler des documents contenant des renseignements personnels;
- 2.1.5. Une personne qui s'immisce dans une banque de données contenant des renseignements personnels afin de les altérer.

2.2. Renseignement personnel : Les renseignements personnels sont ceux qui portent sur une personne physique et permettent de l'identifier. Ils sont confidentiels. Sauf exceptions, ils ne peuvent être communiqués sans le consentement de la personne concernée. Un renseignement personnel correspond par exemple à un nom, une adresse physique ou électronique, un numéro de téléphone, une date de naissance, un numéro d'assurance sociale, une plaque d'immatriculation, des photos, des empreintes digitales, un appel passé sur un téléphone intelligent, une connexion à Internet, un historique médical, des transactions

financières. Un individu peut être identifié directement, à l'aide d'un renseignement personnel concret comme son nom, ou indirectement en établissant son profil, à l'aide d'un renseignement personnel plus abstrait comme un critère socioéconomique, psychologique ou idéologique.

2.3. Préjudice sérieux **:** qui porter atteinte à la personne concernée ou à ses biens et nuit à ses intérêts de manière non négligeable. Il peut conduire, par exemple, à l'humiliation, à une atteinte à la réputation, à une perte financière, à un vol d'identité, à des conséquences négatives sur un dossier de crédit, à une perte d'emploi.

3. CADRE JURIDIQUE

La présente procédure est élaborée en tenant compte notamment du cadre juridique suivant :

a) *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (chapitre A-2.1);
b) *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (Loi 25);
c) *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, chapitre G-1.03) Charte des droits et libertés de la personne* (L.R.Q., c. C – 12);
d) *Code civil du Québec* (L.Q. 1991, c. 64);
e) *Loi concernant le cadre juridique des technologies de l'information* (chapitre C-1.1);
f) *Politique sur la sécurité de l'information* du Collège;
g) Règlementation du Collège.

Les articles 63.8 à 63.11 de la Loi sur l'accès permettent de définir ce qu'est un incident de confidentialité et indiquent la marche à suivre lorsque survient un tel incident impliquant un renseignement personnel. Ils prévoient les éléments que l'organisme public visé doit prendre en compte, lorsqu'il évalue le risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné par un incident de confidentialité. Ces articles mentionnent également l'obligation, pour les organismes publics, de tenir un registre de ces incidents. L'article 127.2 de la Loi sur l'accès octroie certains pouvoirs à la Commission d'accès à l'information (CAI) lors d'un tel incident.

4. CHAMP D'APPLICATION

La présente procédure s'applique à l'ensemble des membres du personnel du Collège, qui sont tous concernés par la protection des renseignements personnels détenus collectés, conservés ou communiqués par le Collège, que ces renseignements appartiennent à des membres du personnel, actuels ou anciens, des membres de la population étudiante, actuels ou anciens, ou toute autre personne. Elle s'applique aussi à toute personne liée au Collège et ayant connaissance d'un incident de confidentialité (membres du conseil d'administration, membre d'un comité, population étudiante, contractant, par exemple.).

En cas d'incident, les intervenants ci-dessous sont directement visés par la procédure.

5. RÔLES ET RESPONSABILITÉS

5.1 Responsable de la protection des renseignements personnels (RPRP):

5.1.1 Reçoit les signalements d'incident de confidentialité;

5.1.2 Traite avec empressement les messages reçus dans la boite de courriel prp@bdeb.qc.ca;
5.1.3 Réunit les intervenants en cas d'incident de confidentialité;
5.1.4 Coordonne l'enquête et la mise en place des mesures d'atténuation;
5.1.5 Documente l'incident ou délègue cette responsabilité à un intervenant;
5.1.6 Transmet l'avis d'incident à la CAI lorsque requis (préjudice sérieux) (annexe 1);
5.1.7 Transmet l'avis aux personnes susceptibles de diminuer le préjudice, le cas échéant;
5.1.8 Inscrit la communication de renseignements prévu en 5.1.7 dans le registre des communications prévu par la LAI;
5.1.9 Inscrit l'incident au registre des incidents de confidentialité prévu par la Loi sur l'accès.

5.2 Direction des ressources informationnelles et des technologies numériques (DRITN) en collaboration avec l'analyste en sécurité et la responsable des archives:

5.2.1 Effectue les tâches mentionnées ci-dessus en 5.1.4, 5.1.5 et 5.1.7 lorsque l'incident est de nature technologique. Participe au processus de traitement comme intervenant dans les autres cas;
5.2.2 L'analyste en sécurité et la responsable des archives collaborent au traitement des incidents, aux mesures de mitigation à mettre en place et à la gestion des risques;
5.2.3 L'analyste en sécurité de l'information s'assure de la coordination des actions à prendre en vertu de la *Procédure de gestion des incidents*, dédiée à la gestion des incidents de sécurité (ayant un impact sur la confidentialité, l'intégrité ou la disponibilité des données ou des systèmes du Collège).

5.3 Direction adjointe aux services des communications :

5.3.1 Collabore au traitement des incidents, particulièrement quant aux communications requises concernant les mesures de mitigation à mettre en place et à la gestion des risques pour le Collège.

5.4 Direction(s) concernée(s) par l'incident :

5.4.1 Collabore(nt) au traitement des incidents;
5.4.2 Transmet(tent) l'avis aux personnes concernées par l'incident (annexe 2);
5.4.3 Transmet(tent) les avis aux contractants lorsque requis contractuellement.

6. DOCUMENTS

Formulaire de déclaration d'incident de sécurité portant atteinte à des renseignements personnels de la CAI

7. PROCÉDURE DE TRAITEMENT DES INCIDENT DE CONFIDENTIALITÉ

7.1 Signalement, traitement et évaluation du préjudice relatif à un indicent de confidentialité

7.1.1. Tout incident de confidentialité doit être signalé sans délai à la personne responsable de la protection des renseignements personnels (RPRP) par la direction détentrice du renseignement personnel concerné ou, à défaut, par toute autre personne qui a connaissance de cet incident;
7.1.2. La RPRP, qui a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel détenu par le Collège, réunit les intervenants concernés (voir article 5);

7.1.3. La RPRP, ou une personne qu'elle désigne, documente l'incident avec la collaboration des intervenants, en menant une enquête appropriée et impartiale sur:
- 7.1.3.1. Les circonstances de l'incident;
- 7.1.3.2. La date ou la période où est survenu l'incident;
- 7.1.3.3. Les renseignements personnels visés (classer par type s'il y en a plusieurs)
- 7.1.3.4. Les personnes visées;
- 7.1.3.5. Le problème survenu;
- 7.1.3.6. La nature du préjudice, et s'il est survenu ou s'il peut encore être évité ou cessé;
- 7.1.3.7. Les mesures de mitigation immédiates à prendre (diminution du préjudice causé et éviter que l'incident ne se reproduise). Par exemple :
  - 7.1.3.7.1. Ligne d'assistance dédiée à la gestion de l'incident (prp@bdeb.qc.ca);
  - 7.1.3.7.2. Accès (gratuit si approprié) à des services de surveillance du crédit;
  - 7.1.3.7.3. Désignation d'une personne chargée de répondre aux questions des personnes concernées;
- 7.1.3.8. L'évaluation du préjudice. Le préjudice est-il sérieux ? Prise en compte des facteurs suivants pour cette évaluation:
  - 7.1.3.8.1. La sensibilité des renseignements visés (renseignement d'identité, financier, médical, disciplinaire, etc.);
  - 7.1.3.8.2. Les conséquences appréhendées (vol d'identité, fraude financière, atteinte importante à la vie privée);
  - 7.1.3.8.3. La probabilité de l'utilisation à des fins préjudiciables (voir article 2.3).

7.2 En cas de risque de préjudice sérieux :

7.2.1. La RPRP avise la Commission d'accès à l'information avec empressement[1] (la CAI peut aider à traiter l'incident)
- 7.2.1.1. L'avis contient les renseignements prévus à l'annexe 1 et se fait via le *Formulaire de déclaration d'incident de sécurité portant atteinte à des renseignements personnels* de la CAI. Le Collège doit transmettre[2] avec diligence à la CAI tout renseignement prévu à cette annexe dont le Collège prend connaissance après lui avoir transmis l'avis;
- 7.2.1.2. Si un préjudice sérieux résulte de l'incident, la CAI peut ordonner au Collège d'aviser les personnes concernées, s'il ne le fait pas;
- 7.2.1.3. La CAI peut ordonner à toute personne d'appliquer les mesures jugées pertinentes afin de protéger les droits des personnes concernées;
- 7.2.1.4. La CAI peut ordonner la remise des renseignements personnels impliqués dans l'incident au Collège, de même que leur destruction.

7.2.2. La direction concernée avise directement les personnes concernées, par tout moyen :
- 7.2.2.1. Sauf si cet avis est susceptible d'entraver une enquête faite par une personne ou par un organisme qui, en vertu d'une loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois;
- 7.2.2.2. L'avis contient les renseignements prévus à l'annexe 2;
- 7.2.2.3. À compter du moment où l'avis aux personnes concernées n'est plus susceptible d'entraver une telle enquête, celles-ci sont avisées;

[1] Pour trouver le formulaire : site de la Cai : Incident de sécurité impliquant des renseignements personnels | Commission d'accès à l'information du Québec (gouv.qc.ca) Télécharger le formulaire de la CAI au : CAI_FO_decl_incident_securite.docx (live.com)

[2] Adresse de la CAI : Commission d'accès à l'information, 525, boulevard René-Lévesque Est, Bureau 2.36. Québec (Québec) G1R 5S9 Téléphone sans frais : 1 888 528-7741 - Télécopieur : 418 529-3102 - Courrier électronique : cai.communications@cai.gouv.qc.ca

7.2.2.4. L'avis peut être indirect (avis public par tout moyen dont on peut raisonnablement s'attendre à ce qu'il permette de joindre la personne concernée) si le fait de le transmettre directement pourrait causer un préjudice accru à la personne concernée;

7.2.2.5. L'avis peut également être indirect lorsque le fait de transmettre l'avis est susceptible de représenter une difficulté excessive pour l'organisation ou lorsque le Collège n'a pas les coordonnées de la personne concernée;

7.2.2.6. Le Collège demeure toutefois ensuite tenu de transmettre, avec diligence, un avis direct à la personne concernée lorsqu'il est en mesure de le faire et qu'aucune des exceptions mentionnées ne s'applique à la situation.

7.2.3. La RPRP ou la direction concernée avise une personne ou organisme susceptible de diminuer le préjudice, si opportun;

7.2.3.1. Cette communication (nécessaire) est inscrite dans le registre des communications requis par la Loi sur l'accès par la RPRP en vertu de l'article 63.8 al. 2 LAI.

7.3. Mesures de mitigation additionnelles. La RPRP avec la collaboration des intervenants, détermine si d'autres mesures de mitigation peuvent être mises en place afin de réduire les préjudices et d'éviter qu'un tel incident ne se reproduise. Par exemple :

7.3.1.1. Renégocier les ententes contractuelles avec des tiers;
7.3.1.2. Changer de fournisseur de services;
7.3.1.3. Restreindre l'accès aux renseignements personnels;
7.3.1.4. Former adéquatement les membres du personnel;
7.3.1.5. Souscrire à une police d'assurance contre les cyber-risques;
7.3.1.6. Modifier les politiques internes;
7.3.1.7. Mettre à jour les solutions technologiques, avec, si nécessaire, l'intervention de consultants externes (ex : sécurité de l'information).

7.4. Clauses contractuelles. Les directions avisent leur contractant si des clauses contractuelles le prévoient et sont applicables.

7.5 Registre des incidents de confidentialité

7.5.1. La RPRP inscrit l'incident de confidentialité (même s'il ne présente pas de préjudice sérieux pour les personnes concernées) au registre requis par la loi en vertu de l'article 63.11 LAI;
7.5.2. La CAI peut consulter l'information colligée au registre et une copie doit lui être transmise à sa demande;
7.5.3. Le registre contient les renseignements prévus à l'annexe 3;
7.5.4. Le registre doit être conservé pendant une période de 5 ans après la date ou la période au cours de laquelle le Collège a pris connaissance de l'incident.

8. RÉVISION DU PROCESSUS EN CONTINU

8.1. Informer et rappeler à la communauté du Collège, et plus particulièrement aux membres du personnel dont les fonctions sont plus à risque d'incident de confidentialité, de la définition d'incident de confidentialité et de leur obligation d'aviser la personne responsable de la protection des renseignements personnels de tout incident de confidentialité survenu.

Par exemple :

- Sensibiliser lors des rencontres du personnel;
- Article dans le BdeB Mag;
- Rappel dans la signature courriel du RAIPRP;
- Prévoir des formations
- Établir des procédures opérationnelles identifiant les risques et les moyens de les atténuer.

8.2. Lorsque les vulnérabilités son identifiées, déterminer les solutions à implanter pour corriger celles-ci et réaliser des tests afin de s'assurer que les mesures de correction sont efficaces;

8.3. En faire rapport à la direction générale;

8.4. Effectuer les communications requises internes et externes, le cas échéant;

8.5. Effectuer des exercices de simulation des actions à prendre en cas d'incident de confidentialité.

9. ENTRÉE EN VIGUEUR

La présente procédure entre en vigueur le 22 septembre 2022.

ANNEXES

Annexe 1 **– Avis à transmettre à la CAI en cas de préjudice sérieux**

Le Collège doit aviser, avec diligence et par écrit, la Commission qu'un incident de confidentialité présente un risque qu'un préjudice sérieux soit causé. Il doit aussi transmettre tout renseignement dont il prend connaissance après avoir transmis un avis initial, avec diligence à compter de la connaissance. L'avis doit, dans la mesure où ils sont connus, contenir les renseignements suivants :

1. le nom du Collège comme ayant fait l'objet de l'incident de confidentialité;
2. le nom et les coordonnées de la personne à contacter au sein du Collège relativement à l'incident;
3. une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;
4. une brève description des circonstances de l'incident et, si elle est connue, sa cause;
5. la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;
6. la date ou la période au cours de laquelle le Collège a pris connaissance de l'incident;
7. le nombre de personnes concernées par l'incident et, parmi celles-ci, le nombre de personnes qui résident au Québec ou, s'ils ne sont pas connus, une approximation de ces nombres;
8. une description des éléments qui amènent l'organisation à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées, tels que la sensibilité des renseignements personnels concernés, les utilisations malveillantes possibles de ces renseignements, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables;
9. les mesures que le Collège a prises ou entend prendre afin d'aviser les personnes dont un renseignement personnel est concerné par l'incident, de même que la date où les personnes ont été avisées ou le délai d'exécution envisagé;
10. les mesures que le Collège a prises ou entend prendre à la suite de la survenance de l'incident, notamment celles visant à diminuer les risques qu'un préjudice soit causé ou à atténuer un tel préjudice et celles visant à éviter que de nouveaux incidents de même nature ne se produisent, de même que le délai où les mesures ont été prises ou le délai d'exécution envisagé;
11. le cas échéant, une mention précisant qu'une personne ou un organisme situé à l'extérieur du Québec et exerçant des responsabilités semblables à celles de la Commission à l'égard de la surveillance de la protection des renseignements personnels a été avisé de l'incident.

Annexe 2 **– Avis à transmettre aux personnes concernées par l'incident de confidentialité en cas de préjudice sérieux**

L'avis devant être transmis à la personne dont un renseignement personnel est concerné par un incident qui présente un risque qu'un préjudice sérieux soit causé doit contenir les renseignements suivants :

1. une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;
2. une brève description des circonstances de l'incident;
3. la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;
4. une brève description des mesures que le Collège a prises ou entend prendre à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé;
5. les mesures que le Collège suggère à la personne concernée de prendre afin de diminuer le risque qu'un préjudice lui soit causé ou afin d'atténuer un tel préjudice;
6. les coordonnées permettant à la personne concernée de se renseigner davantage relativement à l'incident.

Annexe 3 **– Contenu du registre requis concernant les incidents de confidentialité**

1. Une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;
2. Une brève description des circonstances de l'incident;
3. La date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;
4. La date ou la période au cours de laquelle le Collège a pris connaissance de l'incident;
5. Le nombre de personnes concernées par l'incident ou, s'il n'est pas connu, une approximation de ce nombre;
6. Une description des éléments qui amènent le Collège à conclure qu'il existe ou non un risque qu'un préjudice sérieux soit causé aux personnes concernées, tels que la sensibilité des renseignements personnels concernés, les utilisations malveillantes possibles de ces renseignements, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables;
7. Si l'incident présente un risque qu'un préjudice sérieux soit causé, les dates de transmission des avis à la Commission et aux personnes concernées, de même qu'une mention indiquant si des avis publics ont été donnés par l'organisation et la raison pour laquelle ils l'ont été, le cas échéant;
8. Une brève description des mesures prises par l'organisation, à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé.