Politique du Séminaire de Chicoutimi - Services éducatifs quant à la protection des renseignements personnels de ses élèves, de leurs parents et de son personnel

PRÉAMBULE Pour accomplir ses missions le Séminaire de Chicoutimi est amené à collecter et traiter des données personnelles des élèves et de leurs responsables. Ces données sont recueillies soit lors de l'inscription de l'élève, de sa réinscription ou plus généralement tout au long de son parcours scolaire. Le Séminaire de Chicoutimi est soucieux de la protection des données personnelles qui lui sont confiées et applique des règles et procédures visant à garantir le respect de la confidentialité des informations traitées par ses services. Ainsi, le Séminaire de Chicoutimi a mis en place la présente politique, conformément à la réglementation actuelle et plus particulièrement à la Loi 25 (Loi modernisant des dispositions législatives en matière de protection des renseignements personnels). Cette politique fera l'objet de mises à jour régulières, au gré des dispositions impératives qui entreront progressivement en vigueur en 2023 et 2024 et pourra être consulté sur le site internet de l'établissement.

1- Personnes responsables

La personne désignée responsable de la protection des renseignements personnels au sein du Séminaire de Chicoutimi est :

Madame Bianca Tremblay, directrice générale;
bianca.tremblay@sdec.education

Toute question ou plainte en relation avec la protection des données personnelles doit être adressée à cette personne par courriel.

En cas d'empêchement de cette personne, la Coordonnatrice du Service d'accueil et d'encadrement, **M^{me} Sara Belley**, du Séminaire sera le référent et peut être joint à l'adresse courriel suivante : **sara.belley@sdec.education**

Leurs coordonnées sont en tout temps consultables sur le site internet du Séminaire.

Un Comité interne de suivi de la politique de la confidentialité et la protection des renseignements personnels des élèves, de leurs parents et de son personnel est constitué pour traiter les cas éventuels d'incident, réviser la politique pour la mettre en conformité avec les impératifs de la Loi et pour effectuer une reddition de comptes.

Ce comité est composé de :

- ➔ De la directrice générale;
- ➔ De la Coordonnatrice du Service d'accueil et d'encadrement;
- ➔ D'un représentant des finances;
- ➔ De la Coordonnatrice des Communications;
- ➔ D'un conseiller pédagogique;
- ➔ Du Responsable de la vie scolaire;
- ➔ Du Coordonnateur des ressources matériels;

Le Comité dispose de la possibilité d'inviter toute personne utile aux débats.

Un document précisant les rôles et responsabilités est partagé à l'annexe A.

2- Procédure en cas d'incident

En cas d'incident de confidentialité impliquant un renseignement personnel, la procédure interne de traitement d'un incident de confidentialité est déclenchée, le schéma de traitement figure à l'annexe B (Grille d'analyse – Évaluation des risques de préjudice).

Au terme de cette procédure, si l'existence d'un incident est établie et qu'un risque de préjudice sérieux est avéré :

- ➔ Les personnes concernées sont immédiatement avisées;
- ➔ La Commission d'accès à l'information du Québec est informée, via le formulaire officiel figurant à l'annexe C;
- ➔ L'incident est consigné dans le registre des incidents, sous la responsabilité du Comité interne et une copie doit être transmise à la Commission à sa demande.

Dans tous les cas de signalement, le Comité interne est réuni :

- ➔ Pour statuer sur les mesures raisonnables à prendre pour diminuer les risques qu'un préjudice soit causé aux personnes concernées et éviter que de nouveaux incidents de même nature ne se produisent;
- ➔ Pour proposer au besoin la révision des processus internes.

3- Données collectées

Relatives aux élèves et à leurs responsables

Sont considérées comme personnelles toutes les données qui, individuellement ou collectivement permettent d'identifier directement ou indirectement les personnes, notamment, sans que la liste ci-dessous ne puisse être considérée comme exhaustive :

- ➔ Données d'identité : date et lieu de naissance, langues parlées, établissement d'origine, identité des parents et de la fratrie, données relatives à la situation de la famille, pour les tarifs de fratrie notamment;

- ➔ Données d'ordre pédagogique relatives à la scolarité et aux examens (classes fréquentées, dossier scolaire antérieur à la scolarisation au Séminaire, disciplines étudiées, travaux scolaires, notes, sanctions, sorties scolaires, voyages..., Association sportive, Compétition, etc.);
- ➔ Données logistiques (fréquentation des différents services, activités inter scolaires, activités concentration sportives, artistiques et culturels, camp de jour, etc...);
- ➔ Données financières : pour la facturation de la scolarité et des services fréquentés, pour les attestations relatives à cette facturation (numéros NAS notamment);
- ➔ Données santé : fiche médicale, fiches d'accidents, plans d'interventions;
- ➔ Données sécurité : coordonnées des familles;
- ➔ Données visuelles et numériques : photos, vidéos, exposés;
- ➔ Données d'accès au portail : codes, identifiants, mots de passe;
- ➔ Données obligatoires à transmettre au ministère de l'Éducation et tous les documents obligatoires pour les subventions.

Ces données sont recueillies soit lors de l'inscription de l'élève, de sa réinscription ou plus généralement tout au long de son parcours scolaire par le biais de formulaires adressés aux familles.

En tout état de cause, le Séminaire de Chicoutimi veille à ce que seules soient collectées, traitées et conservées, les données obligatoires, adéquates et pertinentes au regard de ce qui est nécessaire à la poursuite des finalités poursuivies par le Séminaire de Chicoutimi pour répondre à ses missions.

<u>Relatives aux membres du personnel</u>

Les modalités de traitement des données relatives aux personnels feront l'objet d'un document distinct.

Supports dans lesquels peuvent être collectées et stockées ces données :

- ➔ COBA (pour la gestion administrative des élèves, des inscriptions et de la facturation, mais aussi pour les achats et la paie);
- ➔ Site internet du Séminaire de Chicoutimi;

- ➔ Serveurs informatiques et sauvegardes externes;
- ➔ Sauvegardes des caméras de surveillance.

4- Usage

Protection et sécurité des données

- ➔ L'accès au Portail Parents se fait via une connexion sécurisée;
- ➔ L'utilisation du réseau est surveillée et une détection des intrusions ainsi qu'un antivirus sont en place;
- ➔ Les sauvegardes sont encryptées et ne peuvent être restaurées qu'à partir de la plateforme;
- ➔ Elles ne sont transmises que partiellement aux tiers et dans les cas strictement nécessaires et autorisées.

Accessibilité des données

Services internes au Séminaire de Chicoutimi

Plusieurs services internes au Séminaire de Chicoutimi ont accès aux données. Des accréditations internes veillent au respect de la confidentialité des données, ainsi, des profils d'utilisateur garantissent aux familles l'accès aux informations uniquement par les services concernés. À titre d'exemple, les données relatives à la santé ne sont accessibles qu'à l'infirmière, et à l'équipe pédagogique et à toute personne habilitée en interne à disposer de ces renseignements.

De même, les informations financières ne sont accessibles qu'aux services financiers et à l'équipe de direction.

Divulgation des informations personnelles - Transmission aux tiers

Les données personnelles peuvent être transmises par le Séminaire de Chicoutimi :

- ➔ À des tiers, prestataires de service (le plus souvent dans le cadre des services proposés en complément de l'enseignement ou dans le cadre des sorties et voyages scolaires), - aux partenaires

du quotidien de l'établissement (assureur, prestataire informatique, réviseur externe, des intervenants autorisés);

- ➔ Au Ministère de l'Éducation du Québec;
- ➔ À toutes autres institutions (tels que les organismes publics en charge des examens, de l'orientation) à qui ces informations doivent être transmises dans le cadre de la scolarité de l'élève et de son parcours scolaire.

Ce partage de données sera limité au cadre strictement nécessaire et obligatoire, et jamais à des fins commerciales.

L'Établissement s'assurera que les prestataires de service et partenaires du Séminaire de Chicoutimi respectent eux aussi la Loi 25 prennent les précautions appropriées pour protéger les données.

Durée de stockage des données

- ➔ Les données sont conservées le temps nécessaire pour satisfaire aux obligations légales et contractuelles du Séminaire de Chicoutimi;
- ➔ La plupart des données sont utilisées pendant l'année scolaire en cours sur les supports précités puis archivées ou détruites.

5- Droit des usagers

La présente politique garantit aux élèves, à leurs responsables légaux et aux membres du personnel :

- ➔ Que leurs renseignements personnels ne seront pas communiqués sans leur consentement à des fins d'étude, de recherche ou de productions de statistiques et dans le cadre d'une transaction commerciale;
- ➔ Qu'une évaluation des facteurs relatifs à la vie privée sera effectuée avant de communiquer des renseignements personnels sans le consentement des personnes concernées à des fins d'étude, de recherche ou de production de statistiques.

ANNEXE A

Les rôles et responsabilités des membres du comité interne de suivi de la politique de la confidentialité et la protection des renseignements personnels des élèves, de leurs parents et de son personnel:

Membre du comité	**Rôles et responsabilités**
la directrice générale	• Effectuer une vigie sur les utilisateurs des renseignements personnels • Interpeller le comité lors du doute ou de la confirmation d'une fuite d'information • Prendre des mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que d'autres incidents de même nature se produisent. • Aviser la Commission, avec diligence, d'un incident de confidentialité impliquant un renseignement personnel qu'elle détient lorsque l'incident présente un risque qu'un préjudice sérieux soit causé aux personnes concernées; • Transmettre à la Commission, dans les meilleurs délais, tout renseignement complémentaire dont elle prend connaissance après lui avoir transmis le présent avis;
la Coordonnatrice du Service d'accueil et d'encadrement	• Assurer la confidentialité des données relatives à la discipline et à l'encadrement;
la responsable des finances	• Tenir le régistre des incidents de confidentialité • Inscrire l'incident déclaré dans son registre des incidents de confidentialité et communiquer ce dernier à la Commission sur demande.

	• Assurer la confidentialité des données financières et personnelles; • Assurer la saine gestion des accès aux informations financières et personnelles.
la Coordonnatrice des Communications	• Aviser toute personne dont un renseignement personnel a été compromis par un incident de confidentialité si cet incident présente un risque qu'un préjudice sérieux soit causé.
le conseiller pédagogique	• Assurer la confidentialité des données pédagogiques; • Assurer la saine gestion des accès aux informations pédagogiques.
le Responsable de la vie scolaire	• Assurer la confidentialité des données relatives aux inscriptions de la vie scolaire;
le Coordonnateur des ressources matériels	• Assurer la fiabilité de l'hébergement du système informatique. • Assurer la confidentialité des mots de passe. • Offrir des formations sur la sécurité des données personnelles.
Les membres du comité	• Évaluer si un incident de confidentialité représente un risque qu'un préjudice sérieux soit causé aux personnes concernées par l'incident de confidentialité; • Prendre des mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que d'autres incidents de même nature se produisent.

ANNEXE B

Incidents de confidentialité

Grille d'analyse – Évaluation des risques de préjudice

Cette grille vous permet d'évaluer les risques de préjudices lorsqu'un incident de confidentialité se produit dans votre établissement.

Les **risques jugés sérieux ou élevés** doivent être divulgués à la Commission d'accès à l'Information (« CAI ») ainsi qu'aux personnes dont les renseignements personnels sont visés par l'incident de confidentialité.

Notions importantes :

Renseignement personnel (« RP »)
Tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier.

Incident de sécurité
Incident affectant la disponibilité, l'intégrité ou la confidentialité d'un actif informationnel d'un établissement, incluant ou non des renseignements personnels.

Lorsque des renseignements personnels sont touchés par l'incident, il s'agit d'un **incident de confidentialité**

- Accès, utilisation ou communication non autorisé(e) par la loi d'un RP
- Perte d'un RP
- Toute autre atteinte à la protection d'un RP

Renseignements sensibles
Renseignement qui, de par leur nature notamment médicale, biométrique ou autrement intime, ou en raison du contexte de leur utilisation ou communication, suscitent un haut degré d'attente raisonnable en matière de vie privé.

1. **Date ou période de l'évènement : _____**

2. **Type d'incident / Cause de l'incident :**

   ☐ Accès non autorisé
   ☐ Utilisation non autorisée
   ☐ Communication non autorisée
   ☐ Perte ou autre atteinte à la protection des renseignements personnels

3. **Des renseignements personnels sont-ils visés ?**

   ☐ Oui. Il s'agit d'un incident de confidentialité. Compléter les questions subséquentes pour évaluer les risques de préjudice.
   ☐ Non. Il s'agit d'un incident de sécurité. Cependant, vous n'avez pas de déclaration à faire à la CAI. Inscrire l'incident au registre et continuer l'analyse pour évaluer les conséquences appréhendées et les mesures à prendre.

4. **Quels renseignements sont visés :**

   ☐ **Renseignements d'identification**
   Ex. : Nom, coordonnées (adresse postale, courriel, numéro de téléphone), numéro d'assurance sociale / maladie, permis de conduire, code permanent, codes d'utilisateur, mot de passe, etc.

   ☐ **Renseignements démographiques**
   Ex. : Date de naissance, origines ethniques, orientation sexuelle, identité de genre, religion, état matrimonial, niveau d'instruction, etc.

   ☐ **Renseignements de nature financière**
   Ex. : Numéro de carte de crédit, de compte bancaire, information sur le soutien financier ou l'accommodation financière fournie par un établissement à un élève / un employé, salaire, conditions d'emploi, etc.

   ☐ **Renseignements de nature médicale**
   Ex. Âge, taille, poids, dossiers médicaux, groupe sanguin, plan d'intervention, etc.

   ☐ **Renseignement génétique ou biométrique**
   Ex. Empreintes digitales, signature vocale, ADN, etc.

   ☐ **Autre, Préciser _____**

   Ex. Antécédents judiciaires, dossier d'employé, etc.

5. **Les renseignements visés étaient-ils chiffrés / protégés par un mot de passe ?**
   ☐ Oui, passez à la question 9
   ☐ Non, continuez l'analyse

6. **Ont-ils été récupérés ou détruits ?**
   ☐ Oui, passez à la question 9
   ☐ Non, continuez l'analyse

7. **Quelles sont les mesures qui ont été prises pour réduire les risques ?**
   Ex. Mesures de sécurité administratives, physiques, techniques, contact avec les autorités policières ou des experts externes, etc.

8. **Combien de personnes sont visées (Élèves, parents, employés actuels ou antérieurs, consultants)**

9. **Des conséquences peuvent-elles néanmoins être appréhendées ? :**
   ☐ Oui, continuez l'analyse
   ☐ Non, vous n'avez pas de déclaration à faire à la CAI, mais vous devez inscrire l'incident au registre

10. **Quelles sont les conséquences appréhendées de l'utilisation du RP :**
    ☐ Vol d'identité
    ☐ Fraude financière / Impact sur le dossier de crédit
    ☐ Diffusion des renseignements personnels, notamment sensibles
    ☐ Répercussion sur la santé physique ou psychologique
    ☐ Perte d'emploi
    ☐ Humiliation, atteinte à la réputation, à la vie privée
    ☐ Impact sur les relations professionnelles ou d'affaires
    ☐ Autre, précisé _____

11. **Quelles sont les probabilités de l'utilisation du RP à des fins préjudiciables :**
    ☐ Faible
    ☐ Moyen
    ☐ Élevé

12. **En fonction de cette évaluation (*niveau du préjudice, du type de renseignements personnels visés, des mesures prises, de la probabilité que les conséquences appréhendées se réalisent, l'incident de confidentialité doit* *(plus d'un choix peut s'appliquer)* :**
    ☐ Être inscrit au registre des incidents de confidentialité
    ☐ Être déclaré avec diligence à la CAI (formulaire)
    ☐ Être déclaré aux personnes concernées*

    ***Note :** La personne concernée n'a pas à être avisée si cela est 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.*

    Signature de la personne ayant fait l'évaluation :

    Signature du responsable PRP :

Commission d'accès à l'information du Québec

ANNEXE C

Section réservée à la Commission
Numéro de référence : _____
Date de réception : ___ / ___ / _____

AVIS À LA COMMISSION D'ACCÈS À L'INFORMATION

CONCERNANT UN INCIDENT DE CONFIDENTIALITÉ IMPLIQUANT DES RENSEIGNEMENTS PERSONNELS ET QUI PRÉSENTE UN RISQUE DE PRÉJUDICE SÉRIEUX

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels
Loi sur la protection des renseignements personnels dans le secteur privé

Objet du présent formulaire

Ce formulaire vise à permettre aux organisations[1] d'aviser la Commission d'accès à l'information (la Commission) de tout incident de confidentialité impliquant un renseignement personnel qu'elles détiennent et présentant un risque de préjudice sérieux.

On entend par « incident de confidentialité » :

- l'accès non autorisé par la loi à un renseignement personnel;
- l'utilisation non autorisée par la loi d'un renseignement personnel;
- la communication non autorisée par la loi d'un renseignement personnel;
- la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

Assurez-vous de ne pas transmettre de renseignements personnels permettant d'identifier une personne dans ce formulaire et dans tout autre document que vous transmettrez à la Commission.

Soyez avisé que les informations inscrites dans le présent formulaire sont soumises à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. Ainsi, certains renseignements, dont le nom de votre organisation et le fait qu'un incident l'impliquant est survenu, pourraient être communiqués publiquement.

Si vous manquez d'espace dans l'un des champs, joignez une annexe présentant l'ensemble de votre réponse lorsque vous transmettez le formulaire à la Commission et inscrivez « Voir annexe » dans le champ concerné.

Vous pouvez transmettre le formulaire et les documents joints par courrier électronique, par la poste ou par télécopieur aux coordonnées suivantes :

Commission d'accès à l'information
525, boulevard René-Lévesque Est, Bur. 2.36
Québec (Qc) G1R 5S9
Téléphone : 418 528-7741 – Sans frais : 1 888 528-7741 – Télécopieur : 418 529-3102
Courrier électronique : cai.communications@cai.gouv.qc.ca

[1] On entend par « organisation » : organisme public, personne qui exploite une entreprise, ordre professionnel, parti politique, député indépendant ou candidat indépendant, syndicat, association, organisme à buts non lucratifs, travailleur autonome et pigiste.

Commission d'accès à l'information du Québec

Obligations de l'organisation

- ✓ Évaluer si un incident de confidentialité représente un risque qu'un préjudice sérieux[2] soit causé aux personnes concernées par l'incident de confidentialité;
- ✓ Prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que d'autres incidents de même nature se produisent. Le fait de déclarer un incident de confidentialité à la Commission ne dispense pas une organisation de cette obligation;
- ✓ Aviser toute personne dont un renseignement personnel a été compromis par un incident de confidentialité si cet incident présente un risque qu'un préjudice sérieux soit causé. En cas de défaut, la Commission pourrait ordonner de le faire;
- ✓ Aviser la Commission, avec diligence, d'un incident de confidentialité impliquant un renseignement personnel qu'elle détient lorsque l'incident présente un risque qu'un préjudice sérieux soit causé aux personnes concernées;
- ✓ Transmettre à la Commission, dans les meilleurs délais, tout renseignement complémentaire dont elle prend connaissance après lui avoir transmis le présent avis;
- ✓ Inscrire l'incident déclaré dans son registre des incidents de confidentialité et communiquer ce dernier à la Commission sur demande.

Vous pouvez obtenir plus de renseignements au sujet de vos obligations en matière d'incident de confidentialité impliquant des renseignements personnels sur notre site Web à l'adresse https://www.cai.gouv.qc.ca/incident-de-confidentialite-impliquant-des-renseignements-personnels/

Rôle de la Commission au regard des incidents de confidentialité

- La Commission s'assure que l'organisation respecte ses obligations légales lors d'un incident de confidentialité et qu'elle met en place les mesures nécessaires pour éviter que de nouveaux incidents de même nature ne se produisent.
- La Commission n'accompagne pas l'organisation dans la gestion des incidents de confidentialité.
- La Commission ne procède pas à la validation des mesures prises par l'organisation pour diminuer les risques qu'un préjudice soit causé ou pour éviter que de nouveaux incidents de même nature se produisent.
- Le fait d'aviser la Commission d'un incident de confidentialité ne peut servir à établir la conformité des pratiques d'une organisation à l'égard de ses obligations légales.

[2] Le préjudice sérieux n'a pas à s'être matérialisé. Il peut seulement être susceptible de se produire.

Commission d'accès à l'information du Québec

1. Identification de l'organisation concernée par l'incident de confidentialité
(Veuillez remplir la section A pour un organisme public et la section B pour une entreprise)

A. Identification de l'organisme public

Nom :	
Adresse :	
Personne à contacter relativement à l'incident	
Nom :	Fonction :
Téléphone :	Courriel :
Personne responsable de la protection des renseignements personnels ☐ **Même que précédent**	
Nom :	Fonction :
Téléphone :	Courriel :

B. Identification de l'entreprise

Nom :	
Adresse du siège social :	
Numéro d'entreprise au Québec (selon le Registraire du Québec) :	
Dirigeant principal	
Nom :	Titre / fonction :
Téléphone :	Courriel :
Personne à contacter relativement à l'incident ☐ **Même que précédent**	
Nom :	Fonction :
Téléphone :	Courriel :
Personne responsable de la protection des renseignements personnels ☐ **Même que précédent**	
Nom :	Fonction :
Téléphone :	Courriel :

Commission d'accès à l'information du Québec

2. Date et période de l'incident de confidentialité

Date de l'incident :	Date de découverte de l'incident :
L'incident a eu lieu sur une période de :	

3. Type d'incident de confidentialité

- ☐ Accès non autorisé par la loi à un renseignement personnel
- ☐ Utilisation non autorisée par la loi d'un renseignement personnel
- ☐ Communication non autorisée par la loi d'un renseignement personnel
- ☐ Perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement

3.1 Causes et circonstances de l'incident de confidentialité

Selon le type d'incident sélectionné ci-dessus, identifiez la ou les cause(s) de celui-ci :

☐ Altération délibérée	☐ Communication accidentelle	☐ Communication délibérée sans autorisation	☐ Consultation non autorisée
☐ Cyberattaque (virus, logiciel espion, etc.)	☐ Défaillance technique	☐ Destruction accidentelle	☐ Destruction volontaire sans autorisation
☐ Divulgation accidentelle	☐ Divulgation délibérée sans autorisation	☐ Erreur humaine	☐ Hameçonnage (phishing)
☐ Ingénierie sociale	☐ Perte d'accès aux renseignements	☐ Perte de renseignements	☐ Rançongiciel
☐ Utilisation incompatible	☐ Vol de renseignements	☐ Autre Précisez :	

Selon le type d'incident sélectionné ci-dessus, décrivez les circonstances de celui-ci :

Commission d'accès à l'information du Québec

Sur quel(s) support(s) les renseignements personnels étaient-ils conservés au moment de l'incident :	
☐ Ordinateur de bureau	☐ Dispositif amovible électronique
☐ Papier	☐ Clé USB
☐ Serveur	☐ CD
☐ Bande sonore	☐ Téléphone portable
☐ Infonuagique (cloud)	☐ Tablette
☐ Vidéosurveillance	☐ Ordinateur portable
☐ Photo	☐ Autre Précisez :

4. Description des renseignements personnels visés par l'incident de confidentialité

☐ Nom ☐ Prénom	☐ Adresse du domicile	☐ Date de naissance ou ☐ Année ☐ Mois ☐ Jour ☐ Âge
☐ Numéro de téléphone au domicile	☐ Numéro du cellulaire	☐ Adresse courriel personnelle

☐ Numéro de permis de conduire	☐ Numéro d'assurance sociale
☐ Numéro d'assurance maladie	☐ Numéro de passeport
☐ Salaire	☐ Fonction / occupation

☐ Renseignements sur des employés, clients ou bénéficiaires
Précisez :

☐ Renseignements médicaux
Précisez :

☐ Renseignements génétiques
Précisez :

☐ Renseignements scolaires / académiques
Précisez :

☐ Renseignements bancaires / numéro de compte / institution / placements / hypothèque
Précisez :

☐ Numéro de carte de crédit	☐ Numéro d'identification personnel (NIP)	☐ Nom du détenteur	☐ Code de sécurité à trois chiffres
☐ Numéro de carte de débit	☐ Numéro d'identification personnel (NIP)	☐ Nom du détenteur	

☐ Autres renseignements personnels

Précisez :

☐ Impossible de fournir une description des renseignements personnels visés

Expliquez :

5. Personnes concernées par l'incident de confidentialité

Nombre de personnes concernées par l'incident :

Nombre de personnes concernées par l'incident qui résident au Québec :

Si possible, ventilez le nombre de personnes concernées par l'incident selon leur lien avec l'organisation, qu'il s'agisse d'employés, de clients, d'étudiants, de patients, de membres, de bénévoles, de fournisseurs, etc., actuels ou anciens :

6. Évaluation par l'organisation du fait qu'un risque de préjudice sérieux puisse être causé aux personnes concernées par l'incident de confidentialité

Décrivez les éléments amenant l'organisation à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées. Ce risque peut être attribuable au fait qu'il s'agisse de renseignements personnels sensibles ou à la possibilité que ces renseignements soient utilisés à des fins malveillantes ou préjudiciables. Dans ce cas, indiquez les conséquences appréhendées de leur utilisation sur les personnes concernées.

Commission d'accès à l'information du Québec

Décrivez les raisons qui supportent l'existence d'un risque de préjudice sérieux pour les personnes concernées par l'incident.

Le responsable de la protection des renseignements personnels de votre organisation a-t-il été consulté pour procéder à l'évaluation du risque de préjudice?

☐ Oui ☐ Non

7. Avis de l'organisation aux personnes concernées
(Vous pouvez joindre une copie de l'avis transmis aux personnes concernées)

L'organisation a-t-elle avisé les personnes concernées par l'incident de confidentialité?

☐ Non

☐ Oui. L'avis a été fait par :

☐ Lettre transmise par courrier	☐ Courriel	☐ Message texte
☐ Verbal (ex. par téléphone)	☐ En personne	☐ Autre Précisez :

Date de l'avis :

Si les personnes concernées n'ont pas encore été avisées, quelles mesures seront prises par l'organisation afin de le faire?

☐ Lettre transmise par courrier	☐ Courriel	☐ Message texte
☐ Verbal (ex. par téléphone)	☐ En personne	☐ Autre Précisez :

Date de l'avis prévu :

☐ Aucune notification de l'incident aux personnes concernées n'est prévue.

Expliquez :

Commission d'accès à l'information du Québec

7.1 Contenu de l'avis aux personnes concernées

Sélectionnez les éléments contenus dans l'avis transmis aux personnes concernées par l'organisation.

- ☐ Une description des renseignements personnels visés par l'incident
- ☐ Une brève description des circonstances de l'incident
- ☐ La date ou la période où l'incident a eu lieu
- ☐ Une brève description des mesures que l'organisation a prises ou entend prendre, à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé
- ☐ Les mesures que l'organisation 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
- ☐ Les coordonnées permettant à la personne concernée de se renseigner davantage relativement à l'incident

Y a-t-il des personnes concernées par l'incident qui ne seront pas avisées par l'organisation?

- ☐ Non.
- ☐ Oui. Combien :

  Expliquez :

7.2 Avis public aux personne concernées

L'avis aux personnes concernées a-t-il été fait, exceptionnellement, au moyen d'un avis public?

- ☐ Non
- ☐ Oui. Sélectionnez la raison applicable :
  - ☐ Le fait de transmettre l'avis est susceptible de causer un préjudice accru à la personne concernée.

    Expliquez :
  - ☐ Le fait de transmettre l'avis est susceptible présenter une difficulté excessive pour l'organisation.

    Expliquez :
  - ☐ L'organisation n'a pas les coordonnées des personnes concernées.

    Expliquez :

Commission d'accès à l'information du Québec

Par quels moyens l'avis public a-t-il été fait?
☐ Un avis dans les médias Précisez lesquels : Date de diffusion :
☐ Un communiqué de presse Date de diffusion :
☐ Un avis sur le site Web de l'organisation
☐ Une conférence de presse Lieu : Date :
☐ Une publication diffusée dans les médias sociaux Précisez lesquels :
☐ Autre Précisez :
Est-ce que l'organisation a avisé d'autres autorités de protection des renseignements personnels à l'extérieur du Québec?
☐ Commissaire à la protection de la vie privée du Canada
☐ Office of the information and privacy commissioner of Alberta
☐ Office of the information and privacy commissioner of British Columbia
☐ Commissaire à l'information et à la protection de la vie privée de l'Ontario
☐ Autre. Précisez :

Commission d'accès à l'information du Québec

8. Obligation de diminuer le risque de préjudice

Quelles mesures ont été prise dès la découverte de l'incident, notamment afin de réduire les risques de préjudice aux personnes concernées?

Dans quel délai ces mesures ont-elles été prises?

Est-ce que des mesures ont été prises après la découverte de l'incident afin d'éviter que de nouveaux incidents de même nature se reproduisent?

☐ Non
☐ Oui. Précisez :

Y a-t-il des mesures prévues qui n'ont pas encore été prises?

☐ Non
☐ Oui. Précisez :

Indiquez la date de mise en place des mesures prévues :

Une organisation doit transmettre à la Commission tout renseignement relatif à l'incident de confidentialité dont elle prend connaissance après lui avoir transmis le présent avis. L'information complémentaire doit alors être transmise dans les meilleurs délais à compter de cette connaissance.

Est-ce que des informations supplémentaires seront transmises à la Commission concernant l'incident rapporté?

☐ Non
☐ Oui. Précisez lesquelles et indiquez l'échéancier prévu :

Commission d'accès à l'information du Québec

9. Signature

Prénom :	Nom :
Fonction :	Lieu / Ville :
Date de transmission du formulaire à la Commission :	
Pour le compte de : ☐ l'organisme ☐ l'entreprise	
Je déclare que les renseignements concernant l'incident de confidentialité fournis dans la présente déclaration sont complets et conformes aux faits.	
Signature :	