Québec

Fonds de recherche – Nature et technologies
Fonds de recherche – Santé
Fonds de recherche – Société et culture

Directive en cas d'incident de confidentialité impliquant des renseignements personnels

Fonds de recherche du Québec – Nature et technologies
Fonds de recherche du Québec – Santé
Fonds de recherche du Québec – Société et culture

Fonds de recherche du Québec
Nature et Technologies Santé Société et Culture

TABLE DES MATIÈRES

HISTORIQUE DES RÉVISIONS

Cette directive a été modifiée comme suit :

Date	Version	Modification
31 mars 2023	1.0	Entrée en vigueur

OBJET ET PORTÉE

OBJET

La directive en cas d'incident de confidentialité impliquant des renseignements personnels vise à assurer une gestion efficace des incidents de confidentialité par le Fonds de recherche du Québec-Santé, Nature et technologie, Société et culture (les « FRQ »). Par cette directive, les FRQ s'assurent qu'ils sont prêts à prévenir ces incidents, à les détecter et à intervenir le cas échéant. De plus, la directive a pour objectif de limiter les dommages et d'atténuer les risques supplémentaires pour les FRQ et pour les personnes concernées par les renseignements personnels impliqués dans un incident.

La directive définit la structure, les rôles et les responsabilités des membres de l'équipe d'intervention en cas d'incident de confidentialité (EIIC), les types d'incidents impliquant des renseignements personnels et l'approche visant à se préparer, à identifier, à évaluer, à diminuer les risques qu'un préjudice soit causé et à éviter que de nouveaux incidents de même nature ne se produisent.

En cas d'incident de confidentialité impliquant un renseignement personnel qu'ils détiennent et présentant un risque de préjudice sérieux, les FRQ doivent aviser la Commission d'accès à l'information et, sauf exception, les personnes concernées par ces renseignements. Les FRQ doivent également tenir un registre des incidents de confidentialité.

PORTÉE

La directive s'applique aux renseignements personnels détenus par les FRQ, peu importe le support. Cela inclut les renseignements détenus par un tiers pour le compte des FRQ (p. ex. : consultants, mandataires, sous-traitants, fournisseurs tiers, membres des conseils d'administration).

Les membres de l'EIIC ont pour mission de diriger l'intervention en cas d'incident de confidentialité ou d'y prendre part. Ils doivent se familiariser avec cette directive et être prêts à réagir et à collaborer dans le but de minimiser les impacts négatifs sur les FRQ et sur les personnes concernées par l'incident.

La présente directive n'a pas pour but de fournir une liste détaillée de toutes les activités à réaliser pour contrer les incidents de confidentialité impliquant des renseignements personnels.

AUTORITÉ

La responsabilité de la protection des renseignements personnels détenus par les FRQ ou pour leur compte incombe au scientifique en chef du Québec, à titre de premier dirigeant des FRQ. Pendant les périodes au cours desquelles un incident de confidentialité impliquant des renseignements personnels se produit, il confie cette responsabilité à la directrice générale ou au directeur général des FRQ, au directeur ou à la directrice des technologies de l'information lorsque l'incident implique les technologies de l'information et la sécurité informatique, et à la personne responsable de la protection des renseignements personnels. Le scientifique en chef prend également appui sur certaines directions clés ou d'autres entités et personnes désignées pour veiller à la mise en œuvre et à la mise à jour continue de la présente directive.

DÉFINITIONS

Incident de confidentialité : Tout incident impliquant un renseignement personnel, soit l'accès, l'utilisation ou la communication non autorisée, la perte ou toute autre atteinte à la protection d'un renseignement personnel.

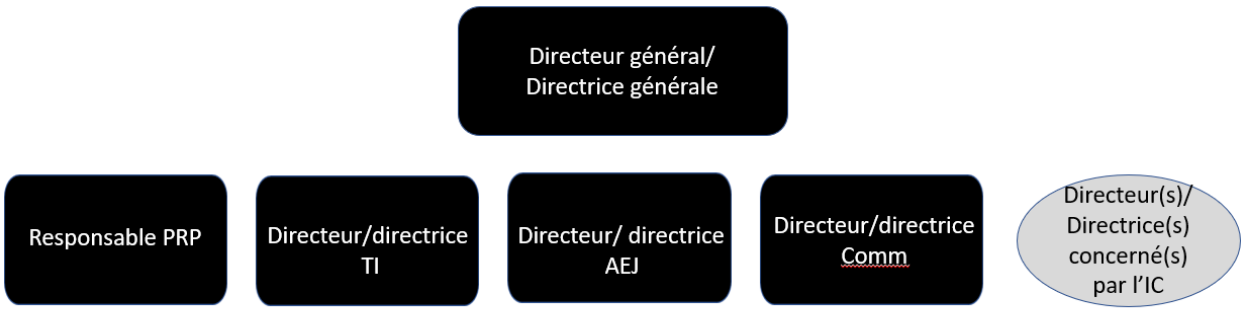
Renseignement personnel : Tout renseignement qui concerne une personne physique et permet, directement ou indirectement, de l'identifier. Parmi ces renseignements, on compte le numéro d'assurance sociale, le numéro d'assurance maladie, les adresses courriel personnelles provenant de l'extérieur des FRQ, le curriculum vitae, etc.

Renseignement personnel sensible : Tout renseignement qui, par sa nature, notamment médicale, biométrique ou autrement intime, ou en raison du contexte de son utilisation ou de sa communication, suscite un haut degré d'attente raisonnable en matière de vie privée.

Risque de préjudice sérieux : Correspond au risque qu'un acte ou qu'un événement soit susceptible de porter atteinte à la personne concernée ou à ses biens et de nuire à ses intérêts de manière sérieuse. Le risque de préjudice sérieux peut être attribuable au fait que l'incident de confidentialité concerne des renseignements personnels sensibles ou à la possibilité que ces renseignements soient utilisés à des fins malveillantes ou préjudiciables.

ÉQUIPE D'INTERVENTION EN CAS D'INCIDENT DE CONFIDENTIALITÉ (EIIC)

STRUCTURE DE L'EIIC



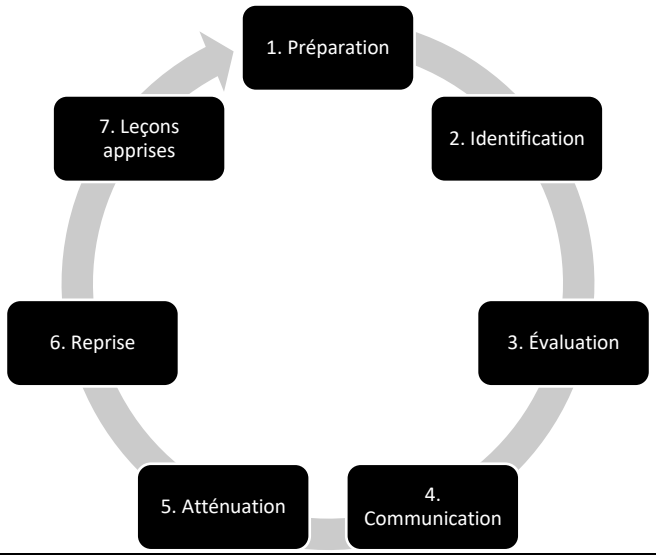
RÔLES DE L'EIIC

Rôle de l'EIIC	Définition du rôle et responsabilités
Directeur ou directrice générale	- Offre un leadership stratégique, une coordination et une surveillance pour toutes les activités de gestion de la sécurité et les contrôles de sécurité des FRQ, y compris ceux liés à la protection des renseignements personnels; - Supervise l'établissement de politiques, de processus et de pratiques à l'échelle des FRQ afin d'assurer une approche intégrée à l'égard de la gestion de la sécurité; - Est la personne Responsable de l'EIIC : réunit l'EIIC et lance le plan d'intervention en cas d'incident. - Est responsable d'assurer les communications internes en lien avec l'incident de confidentialité, notamment avec les membres du personnel.
Directeur ou directrice des technologies de l'information	- Est responsable de la protection de la sécurité de l'information et de la cybersécurité au sein des FRQ; - Supervise l'infrastructure, les réseaux et les applications des TI pour les systèmes des FRQ; - Effectue une veille visant à détecter les incidents de confidentialité à l'aide de contrôles; - En cas d'incident de confidentialité, détermine l'ampleur de l'incident et répertorie les différents systèmes touchés et fait l'inventaire des renseignements personnels concernés; - Fait le lien avec les ministères concernés (ministère de la Cybersécurité et du Numérique et ministère de l'Économie, de l'Innovation et de l'Énergie). -
Directeur ou directrice des affaires éthiques et juridiques (DAEJ)	- Veille à la conformité juridique et normative des politiques et systèmes informationnels des Fonds; - Conseille l'EIIC sur l'interprétation et l'application des lois et des exigences connexes auxquelles les FRQ sont assujettis, et donne des conseils sur l'élaboration de politiques en matière de protection des renseignements personnels et l'interprétation appropriée des exigences législatives en matière de protection des renseignements personnels; - Évalue les répercussions légales lors de la survenance d'un incident de confidentialité; - Agit comme secrétaire de l'EIIC et est ainsi responsable de documenter l'événement du début à la fin. Cette tâche peut être déléguée à un membre du personnel de l'équipe AEJ.
Directeur ou directrice des communications et de la mobilisation des connaissances	- Est responsable des relations publiques; - Doit veiller à ce que les parties prenantes externes, la clientèle des FRQ et le public soient informés en temps opportun et conformément aux pratiques.

Responsable de la protection des renseignements personnels	- Veille à la protection des renseignements personnels au sein des FRQ en conformité avec la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1); - Veille à ce que les renseignements personnels soient protégés et communique toute préoccupation de sécurité en matière de protection des renseignements personnels et sensibles à l'EIIC; - Assure la cohérence et l'harmonisation des interventions entre la sécurité de l'information et la protection des renseignements personnels lors de la mise en œuvre de la directive; - Effectue la vérification des activités en rapport avec la protection des renseignements personnels afin de renforcer les contrôles et la protection des renseignements personnels.
Directeur(s) ou directrice(s) concerné(s) par l'incident	- Collabore avec l'EIIC à mise en œuvre de la présente directive; - Fournit les informations nécessaires à la gestion de l'incident de confidentialité.

CYCLE DE GESTION DES INCIDENTS DE CONFIDENTIALITÉ

Le cycle de gestion des d'incidents de confidentialité impliquant des renseignements personnels débute en amont de la matérialisation d'un incident de confidentialité. L'EIIC complète les étapes suivantes :



Préparation

Durant la phase de préparation, les FRQ :

1. Développent et maintiennent une directive en cas d'incident de confidentialité impliquant des renseignements personnels;

2. Fournissent aux membres du personnel une formation et une sensibilisation régulières en matière de protection des renseignements personnels;
3. Élaborent et mettent en œuvre des mesures physiques, technologiques et administratives en vue de protéger les renseignements personnels;

**Voir l'Annexe A : Liste des mesures préventives que prennent les FRQ pour prévenir les risques ou limiter les risques d'utilisation ou de communication inappropriée de renseignements personnels*

Identification

1. Si un membre du personnel des FRQ a des motifs de croire que s'est produit un incident de confidentialité impliquant des renseignements personnels, il doit en aviser le responsable de l'EIIC sans délai et le processus décrit dans la présente directive est enclenché;

1.1 En cas d'une cyberattaque ou d'un soupçon de cyberattaque, le Plan d'action en cas d'une cyberattaque est activé. Lors de ce processus, s'il y a des motifs de croire que cette cyberattaque implique des renseignements personnels, le processus décrit dans la présente directive est enclenché en parallèle;

2. Le responsable de l'EIIC réunit l'EIIC sans délai;

3. L'EIIC procède à une **évaluation préliminaire de la situation, elle doit définir le contexte de l'incident.**
**Pour ce faire, l'EIIC peut utiliser le formulaire modèle fourni par la Commission d'accès à l'information du Québec (CAIQ). Voir l'Annexe C : Formulaire CAIQ*

3.1 Répertorier les **mesures de sécurité physiques, administratives et informatiques** en place lors de l'incident

---

Évaluation des risques

1. L'EIIC procède à une **évaluation du risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné par un incident de confidentialité et de la gravité du risque.** Le responsable de la protection des renseignements personnels doit participer à cette étape.

**Voir l'Annexe B : Grille des niveaux de gravité*
**Pour ce faire, l'EIIC peut utiliser le formulaire modèle fourni par la CAIQ. Voir l'Annexe C : Formulaire CAIQ*

2. L'EIIC doit déterminer s'il y a ou non un risque de préjudice sérieux.

**Voir l'Annexe D : Liste des éléments que l'EIIC peut considérer pour déterminer s'il y a un risque de préjudice sérieux*

3. L'EIIC décrit **les conséquences appréhendées** de l'utilisation des renseignements personnels pour les personnes concernées.

4. En cas de risque de préjudice sérieux, l'EIIC doit, avec diligence, aviser la CAIQ et les personnes concernées de l'incident.

Communication en cas d'incident – avis aux autorités et aux personnes concernées

L'EIIC :

1. Établit, si nécessaire, un plan de communication pour les communications externes, c'est-à-dire avec les parties prenantes des FRQ et leur communauté;

2. Détermine qui doit être avisé de l'incident de confidentialité, le cas échéant, en fonction de l'évaluation des risques;
   - **2.1** En cas d'incident de confidentialité impliquant un renseignement personnel, la personne concernée doit être avisée en cas de risque de préjudice sérieux;
   - **2.2** Malgré l'article 2.1, une personne dont un renseignement personnel est concerné par l'incident n'a pas à être avisée tant que 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.
   - **2.3** Si requis par leurs engagements contractuels, les FRQ avisent leur le co-contractant visé par l'incident;
   - **2.4** En cas de commission potentielle d'un crime, le service de police concerné doit être avisé (l'EIIC doit alors préserver les éléments de preuve pouvant être pertinents);
   - **2.5** Toute personne ou tout organisme susceptible de diminuer le risque de préjudice (les agences de crédit, un mandataire, un cocontractant, une instance gouvernementale, un syndicat, un ordre professionnel, etc.) peut être avisé. Le cas échéant, seuls les renseignements personnels nécessaires peuvent être communiqués à cette fin sans le consentement de la personne concernée et le responsable de la protection des renseignements personnels des FRQ doit enregistrer cette communication.

3. Désigne les personnes responsables d'aviser les intervenants externes identifiés précédemment ainsi que le moment et le moyen par lequel ils seront avisés (correspondance, courriel, fax, téléphone);

4. Lors de la diffusion des informations concernant l'incident de confidentialité, s'assure de ne pas aggraver le préjudice que pourrait subir les personnes concernées (ex. en limitant au minimum les renseignements personnels dans les avis);

En cas de risque de préjudice sérieux :

5. L'EIIC envoie **un avis à la CAIQ**. Pour ce faire, elle doit remplir le formulaire de la CAIQ prévu à cette fin (Annexe C).

   **Voir l'Annexe E : Liste des éléments que l'avis à la CAI doit comprendre*

6. L'EIIC envoie **un avis aux personnes concernées** conforme aux exigences du *Règlement sur les incidents de confidentialité* et remplit la section pertinente du formulaire de la CAIQ (Annexe C).

   **Voir l'Annexe E : Liste des éléments que l'avis aux personnes concernées doit comprendre*

7. L'avis est transmis directement à la personne concernée par l'incident de confidentialité, sauf lorsque :

   a) Le fait de transmettre l'avis est susceptible de causer un préjudice accru à la personne concernée ;
   b) Le fait de transmettre l'avis est susceptible de représenter une difficulté excessive pour les FRQ (p. ex. l'évaluation des coûts pour le *eDiscovery*, etc.);
   c) Les FRQ n'ont pas les coordonnées de la personne concernée.

8. S'il est nécessaire d'agir rapidement pour réduire le risque de préjudice sérieux ou pour atténuer un tel préjudice, les FRQ peuvent procéder à **un avis public**, à condition qu'un avis direct soit transmis ultérieurement. L'EIIC remplit alors la section pertinente du formulaire de la CAIQ (Annexe C);

9. Le *Règlement sur les incidents de confidentialité* prévoit que les avis doivent être transmis avec **diligence**. Certains délais pour la communication d'avis peuvent être acceptables pour : (i) rassembler les informations pertinentes pour la campagne de notification de la violation, pour (ii) mettre en œuvre des mesures de confinement, et (iii) prendre des dispositions pour la surveillance du crédit ou l'assurance contre le vol d'identité.

10. Dans le cadre de tout incident, si l'EIIC décide de ne pas aviser les personnes concernées et les autres intervenants, identifier et consigner les motifs à l'origine de la décision.

Atténuation – diminuer les risques qu'un préjudice soit causé

Lorsqu'ils ont des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel, les FRQ doivent prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature se produisent.

1. Une fois que les risques auxquels les FRQ sont exposés sont recensés, l'**EIIC** définit et met en place **les mesures que les FRQ entreprendront pour limiter les préjudices et empêcher que l'incident ne cause encore plus de préjudices.**

   L'EIIC doit étudier et lister les stratégies qui peuvent réduire, soit l'impact du risque, soit la probabilité que ce dernier se concrétise, soit les deux en même temps (Voir les exemples à l'Annexe A).

2. L'EIIC doit ensuite réévaluer le niveau de chacun des risques à la lumière des stratégies et des moyens d'atténuation retenus. Tout risque qui persiste une fois que des mesures visant à diminuer ou à éliminer les risques devient un risque résiduel. Les FRQ doivent être en mesure d'assumer la responsabilité des risques résiduels ;

3. L'EIIC doit revoir la proportionnalité de la solution par rapport aux risques encourus. Elle détermine les priorités et identifie les actions à prendre à partir des résultats de l'évaluation de ces risques.

Figure 2 : Cadre de gestion intégré des risques

Reprise, suivi et leçons apprises

Finalement, l'EIIC peut :

1. Tenir une réunion pour discuter des leçons apprises durant la gestion de l'incident de confidentialité;
2. Procéder à une évaluation approfondie de la situation :
    - Approfondir l'analyse des circonstances de l'incident de confidentialité impliquant des renseignements personnels et effectuer une description chronologique des événements et des actions prises face à cet incident, incluant les dates et les intervenants concernés;
    - Répertorier et examiner les normes, politiques ou directives internes en place au moment de l'incident, autant au niveau de la sécurité informatique, lorsque l'information est en cause, et de la protection des renseignements personnels en général;
    - Vérifier si ces normes, politiques ou directives internes ont été suivies par les personnes impliquées – identifier les raisons pour lesquelles elles n'ont pas été suivies, le cas échéant;
    - S'il s'agit d'une erreur de procédure ou d'une défaillance opérationnelle, les consigner au dossier et adapter les processus pour éviter qu'un tel incident ne survienne à nouveau;
    - Formuler les recommandations relatives aux solutions à moyen et long terme et aux stratégies de prévention;
3. Produire un rapport de suivi à partir de l'évaluation approfondie de la situation (Compte rendu de l'incident);
4. Recenser des possibilités d'amélioration pour être mieux préparée;
5. Assurer la responsabilité du suivi des occasions d'amélioration identifiées;
    - Un responsable d'en coordonner la réalisation;
    - Un responsable par action;
    - Des échéances.

6. Les FRQ doivent tenir un **registre** colligeant l'ensemble des incidents de confidentialité impliquant un renseignement personnel qu'ils détiennent, même ceux ne présentant pas de risque de préjudice sérieux. Ce registre décrit les renseignements personnels visés par l'incident et contient des informations sur les circonstances de l'incident, le nombre de personnes visées, l'évaluation de la gravité du risque de préjudice, les mesures prises en réaction à l'incident ainsi que les dates de la survenance de l'incident, de la détection par les FRQ et de la transmission des avis (s'il y a lieu).

RÉVISION ET APPROBATIONS

Les FRQ révisent ce plan sur une base triennale ou suivant des modifications importantes de l'infrastructure informatique et du cadre législatif et réglementaire pertinent.

Annexe A – Mesures préventives des FRQ

Liste des mesures préventives que prennent les FRQ pour prévenir les risques ou limiter les risques d'utilisation ou de communication inappropriée de renseignements personnels :

a) Les FRQ ont adopté une politique de confidentialité, une directive relativement à l'utilisation des outils de travail (mot de passe, sauvegarde) et un énoncé de protection des renseignements personnels;
b) L'ensemble de services infonuagiques, Microsoft 365, utilisé par les FRQ, demande une authentification multifacteur;
c) Les FRQ mettent à jour leurs systèmes et les applications et corrigent les vulnérabilités;
d) Avant d'entreprendre toute collecte d'information, les FRQ définissent les raisons pour lesquelles ils doivent recueillir et utiliser un renseignement personnel.
e) Les FRQ ne recueillent que les seuls renseignements personnels nécessaires à l'exercice des attributions ou à la mise en œuvre d'un programme dont ils ont la gestion.
f) Les FRQ informent adéquatement la personne concernée avant qu'elle fournisse les renseignements personnels attendus.
g) Un renseignement personnel ne sera accessible qu'aux seules personnes ayant la qualité pour le recevoir au sein des FRQ lorsque ce renseignement est nécessaire à l'exercice de leurs fonctions.
h) Un renseignement personnel demeure inaccessible tant que la personne concernée n'a pas consenti à sa divulgation.
i) Les FRQ prennent les mesures de sécurité propre à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de la sensibilité, de la finalité, de la quantité, de la répartition et du support des renseignements personnels.
j) Les FRQ limitent la durée de conservation des renseignements personnels qu'ils conservent et détruisent tout renseignement personnel lorsque l'objet pour lequel il a été recueilli est accompli.

Annexe B – Grille des niveaux de gravité

L'EIIC déterminera la gravité de l'incident. Elle tiendra compte des éléments suivants :

1. Un ou plusieurs systèmes sont affectés;
2. Criticité du ou des systèmes touchés;
3. Touche une ou plusieurs personnes;
4. Touche une seule équipe ou direction, plusieurs équipes ou directions, ou l'ensemble des FRQ.

Le responsable du traitement des incidents doit tenir compte du contexte pertinent (incluant le cycle des programmes aux FRQ, le cheminement des demandes de financement, etc.) et des autres activités en cours pendant l'événement pour bien comprendre les impacts et l'urgence des mesures correctives.

L'EIIC examinera les informations disponibles pour déterminer l'ampleur connue des répercussions par rapport à la taille estimée ainsi que la probabilité de propagation de l'effet et du rythme potentiel de cette propagation. L'EIIC déterminera les répercussions potentielles sur les FRQ, y compris les pertes financières, les dommages à la réputation, et d'autres types de dommages.

L'incident peut être le résultat d'une menace organisée ou non, d'une attaque automatisée ou manuelle, ou encore d'une nuisance ou d'un acte de vandalisme.

Lorsque l'EIIC évalue le risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné par un incident de confidentialité, elle doit considérer notamment la sensibilité du renseignement concerné, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables (voir également la liste de l'Annexe D). Le responsable de la protection des renseignements personnels doit être consulté à cette étape-ci.

Facteurs indiquant un risque plus faible:

- Divulgation accidentelle à une personne et les informations sont récupérées sans utilisation abusive.
- Données cryptées dont la clé de cryptage a été protégée, et il peut être prouvé que la clé de cryptage n'était pas accessible à l'intrus.
- La divulgation était purement interne, les données ont été récupérées et l'organisation a pu utiliser des politiques internes et un système de surveillance pour empêcher toute utilisation abusive.

Pour pouvoir cerner les risques et donc, les mesures de confinement, il faut également identifier les points d'interaction affectés par l'incident dans le parcours du traitement des renseignements personnels :

Les points d'interactions peuvent être

- Les personnes, les ensembles de personnes ou les partenaires et tiers qui accèdent aux renseignements personnels (exemples : employés, clientèle, sous-traitants, firmes de consultation, chercheurs externes, équipes d'entretien de bâtiments ou de systèmes informatiques, fournisseurs de télécommunication);

- Les moyens utilisés pour collecter des renseignements personnels (exemples : formulaires d'abonnement, boîtes courriel, messageries téléphoniques, plateformes collaboratives, sondages, questionnaires);
- Les moyens utilisés pour communiquer des renseignements personnels (exemples : prestations électroniques de service, échanges par courriel, service à la clientèle, sites Web, interfaces d'échange informatisées [API] ou liens électroniques sécurisés);
- Les moyens utilisés pour traiter et conserver des renseignements personnels (exemples: systèmes informatiques, services infonuagiques, copies de sauvegarde, outils de télécommunication, salles et classeurs d'entreposage des dossiers papier).

L'EIIC détermina :

1. s'il y a signes de vulnérabilité dans le système exploité;
2. s'il existe un correctif connu;
3. s'il s'agit d'une nouvelle menace ou d'une menace connue;
4. l'ampleur des mesures pour limiter le problème.

Catégorie	Indicateurs	Portée	Activité
1 - Critique	Perte de renseignements personnels, maliciel	Généralisée ou avec des serveurs critiques, ou perte de données, données volées, accès non autorisé aux données	Actions de l'EIIC, plan d'intervention en cas d'incident, créer un incident de confidentialité, toute l'entreprise
2 – Élevée	Menace théorique qui devient active	Généralisée ou avec des serveurs critiques, ou perte de données, données volées, accès non autorisé aux données	Actions de l'EIIC, plan d'intervention en cas d'incident, créer un incident de confidentialité, toute l'entreprise
3 – Moyenne	Hameçonnage par courriel ou infection par propagation active	Généralisée	Actions de l'EIIC, plan d'intervention en cas d'incident, créer un incident de confidentialité, toute l'entreprise
4 - Faible	Maliciel ou hameçonnage	Hôte individuel ou personne	Aviser l'EIIC, créer un incident de confidentialité

ANNEXE C – Formulaire CAI

Commission d'accès à l'information du Québec

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 :

Commission d'accès à l'information du Québec

☐ 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 :

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 :	

ANNEXE D - Liste des éléments que l'EIIC peut considérer pour déterminer s'il y a un risque de préjudice sérieux:

a) Cause et nature de l'incident (ex. le caractère délibéré ou non de l'incident, l'erreur humaine, une faille informatique, les auteurs connus ou probables de l'incident, l'étendue de la situation : nombre de personnes touchées et secteurs touchés, etc.)
b) Sensibilité des renseignements concernés par l'incident de confidentialité
c) Conséquences appréhendées de leur utilisation
d) Probabilité qu'ils soient utilisés à des fins préjudiciables (en tenant compte, notamment, des mesures de sécurité prises pour les protéger, de leur difficulté d'accès et de leur intelligibilité (mot de passe, encodage, etc.**)**
e) Matérialisation du préjudice/type de préjudice qui pourrait en résulter
f) Longue période d'exposition
g) Mots de passe/ cryptage des données
h) Caractère réversible ou non de la situation (ex. Impossibilité de récupérer les données auprès de destinataires inconnus)
i) Mesures déjà prises pour minimiser le risque (mesures immédiates adéquates pour limiter l'atteinte)
j) Relation entre les destinataires non autorisés et la personne concernée

ANNEXE E – Contenu que prévoit le règlement pour les avis :

Conformément aux exigences du *Règlement sur les incidents de confidentialité*, l'avis à la CAI doit contenir les renseignements suivants :

a) Le nom de l'organisation (avec le numéro d'entreprise du Québec) ;
b) Les coordonnées de la personne à contacter au sein de l'organisation relativement à l'incident ;
c) 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 ;
d) Une description des circonstances de l'incident et, si elle est connue, sa cause ;
e) La date ou la période où l'incident a eu lieu (ou une approximation si cette dernière n'est pas connue) ;
f) La date à laquelle l'organisation a pris connaissance de l'incident ;
g) Le nombre de personnes concernées par l'incident et, parmi celles-ci, le nombre de personnes qui résident au Québec (ou une approximation, si ces nombres ne sont pas connus) ;
h) Une description des éléments qui amènent l'organisation à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées ;
i) Les mesures que l'organisation a prises ou entend prendre afin d'aviser les personnes dont un renseignement personnel est concerné par l'incident ;
j) Les mesures que l'organisation a prises à la suite de la survenance de l'incident, incluant celles visant à diminuer/atténuer les risques qu'un préjudice soit causé et à éviter que de nouveaux incidents de même nature ne se produisent (avec les délais) ;
k) Les coordonnées de la personne à contacter au sein de l'organisation relativement à l'incident.

Conformément aux exigences du *Règlement sur les incidents de confidentialité*, l'avis aux personnes concernées doit contenir les renseignements suivants :

a) 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 ;
b) Une brève description des circonstances de l'incident ;
c) La date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période ;
d) Une brève description des mesures que les FRQ ont prises ou entendent prendre à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé ;
e) Les mesures que la personne concernée peut prendre afin de diminuer/atténuer le risque qu'un préjudice lui soit causé ;
f) Les coordonnées permettant à la personne concernée de se renseigner davantage relativement à l'incident.

ANNEXE F – Exemple de mesures permettant d'éliminer ou de réduire les risques d'atteintes à la vie privée:

a) Prévoir une révision périodique des différentes collectes de renseignements personnels;
b) Mettre en place un système de gestion documentaire qui permet l'application automatisée du calendrier de conservation;
c) Revoir les processus d'attribution et de gestion des accès informatiques;
d) Engager des firmes de sécurité informatique pour revoir périodiquement les paramètres de sécurité de la prestation électronique de service;
e) Revoir les clauses des contrats en matière de confidentialité;
f) Établir un calendrier de formation et d'activités de sensibilisation pour vos employés;
g) Faire une campagne d'information concernant votre nouvelle utilisation des renseignements personnels;
h) Journaliser les accès et exploiter les journaux pour détecter les anomalies;
i) Dépersonnaliser ou anonymiser les renseignements si leur utilisation sous une forme nominative n'est pas requise pour tous.