

A. Contexte

La Financière agricole du Québec (la « **FADQ** ») reconnaît l'importance de protéger les renseignements personnels qu'elle détient. C'est pourquoi elle met en œuvre les moyens technologiques et administratifs nécessaires afin que ceux-ci soient correctement traités tout au long de leur cycle de vie.

Afin de s'acquitter de ses obligations en la matière, la FADQ met en place des mesures de sécurité raisonnables pour protéger les renseignements personnels qu'elle traite, peu importe leur support. Malgré les précautions prises, un incident de confidentialité demeure possible. C'est pourquoi la FADQ se dote d'une Directive sur les incidents de confidentialité impliquant des renseignements personnels (la « **Directive** ») afin de gérer adéquatement ce type d'incident et d'en limiter les conséquences pour les personnes concernées et la FADQ.

B. Objet de la directive

La présente directive poursuit les objectifs suivants :

- Énoncer les obligations de la FADQ à l'égard d'un incident de confidentialité impliquant un renseignement personnel;
- Définir les rôles et les responsabilités des parties prenantes;
- Établir la marche à suivre en cas d'incident.

C. Champ d'application

La présente directive s'applique :

- à tous les employés ainsi que les administrateurs publics de la FADQ ayant connaissance d'un incident de confidentialité impliquant un renseignement personnel détenu par la FADQ;
- aux tiers traitant des renseignements personnels pour le compte de la FADQ et ayant connaissance d'un incident de confidentialité relatif auxdits renseignements.

De plus, la Directive s'applique lorsqu'un incident de sécurité de l'information implique des renseignements personnels, le cas échéant, elle s'intègre au Processus de gestion des incidents de sécurité de l'information de la FADQ qui découle de la Politique de cybersécurité.

D. Cadre légal

Les articles 63.8 à 63.11 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1) (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.

L'article 127.2 de la Loi sur l'accès octroie également certains pouvoirs à la Commission d'accès à l'information (la « **CAI** ») lors d'incident de confidentialité.

Enfin, la Directive tient compte de la réglementation d'application de la Loi sur l'accès.

E. Principes directeurs

Lorsque la FADQ a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'elle détient, elle doit prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de la même nature se produisent.

Dans l'éventualité où des renseignements personnels seraient confiés à des tiers, la FADQ demeure responsable de l'ensemble des obligations en cas d'incident de confidentialité.

F. Définitions

Administrateur public : Les membres du conseil d'administration de la FADQ, dont le président du conseil d'administration et le président-directeur général, ainsi que les vice-présidents de la FADQ.

Cycle de vie : L'ensemble des différentes phases de traitement des renseignements personnels, à savoir leur collecte, leur utilisation, leur communication, leur conservation et leur destruction.

Incident de confidentialité : Tout accès, utilisation ou communication non autorisés par la loi à un renseignement personnel, de même que sa perte ou toute autre forme d'atteinte à sa protection. À titre d'exemples :

- Un employé ou un tiers 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'infiltré dans un système;
- 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;
- Une communication faite par erreur à la mauvaise personne;
- Un employé ou un tiers qui perd ou se fait voler des documents contenant des renseignements personnels;
- Une personne qui s'immisce dans une banque de données contenant des renseignements personnels afin de les altérer ou de les copier.

Incident de sécurité : Un incident de sécurité de l'information se définit comme étant un événement aux conséquences néfastes, prévisibles ou confirmées, sur la disponibilité, l'intégrité ou la confidentialité de l'information relevant de l'autorité d'un organisme public, que sa conservation soit assurée par lui-même ou par un tiers.

Il peut être lié ou non à l'utilisation des technologies de l'information et des communications.

Employés de la FADQ : Tous les employés, réguliers, occasionnels, saisonniers, stagiaires ou étudiants de la FADQ.

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

Renseignement personnel : Toute information qui concerne une personne physique et qui peut permettre de l'identifier :

- directement, c'est-à-dire par le recours à cette seule information ; ou
- indirectement, c'est-à-dire par recoupement avec d'autres informations.

Renseignement personnel non confidentiel : Renseignement personnel auquel la loi ne confère pas un caractère de confidentialité (exemple : les coordonnées professionnelles d'une personne).

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

Ainsi, certains renseignements personnels sont sensibles par leur nature. Il peut s'agir, par exemple, de renseignements médicaux, biométriques, génétiques ou financiers, ou encore de renseignements sur la vie ou l'orientation sexuelle, les convictions religieuses ou bien l'origine ethnique.

Risque plausible de préjudices sérieux : Un acte ou un événement susceptible de porter atteinte à la personne concernée ou à ses biens et de nuire à ses intérêts de manière non négligeable (exemples : humiliation, atteinte à la réputation, perte financière, vol d'identité, conséquences négatives sur un dossier de crédit ou perte d'emploi).

Tiers : Toute personne ou entité extérieures à la FADQ et traitant des renseignements personnels pour le compte de la FADQ (exemple : les consultants externes).

G. Rôles et responsabilités

Chef de la sécurité de l'information organisationnelle, assume la responsabilité de la prise en charge globale de la sécurité de l'information au sein de la FADQ.

Responsable de la protection des renseignements personnels (le « RPRP »), a notamment pour fonction de :

- recevoir les signalements d'incidents de confidentialité;
- traiter le signalement d'incident de confidentialité en collaboration avec les unités administratives concernées;
- transmettre les avis à la CAI;
- collaborer, avec le gestionnaire de l'unité visée, à la transmission d'un avis aux personnes concernées;
- conseiller la FADQ sur les mesures à prendre pour diminuer le risque que de nouveaux incidents de même nature se produisent;
- colliger les informations requises au Registre des incidents de confidentialité; et
- transmettre, sur demande, le Registre des incidents de confidentialité à la CAI.

Gestionnaire, doit notamment :

- sensibiliser et s'assurer du respect et de l'application de la présente Directive dans les unités sous sa responsabilité;
- aviser sans délai le RPRP de tout incident de confidentialité;
- collaborer avec le RPRP au traitement de l'incident, à titre de gestionnaire de l'unité visée par un incident de confidentialité;
- transmettre, en collaboration avec la RPRP, les avis aux personnes concernées;
- appliquer les mesures correctives et préventives.

Employés et tiers, respectent la présente Directive et signalent sans délai tout incident ou suspicion d'incident de confidentialité dont ils ont connaissance au RPRP ainsi qu'à son gestionnaire.

Commission d'accès à l'information, dans le cadre d'un incident de confidentialité, la CAI peut ordonner à toute personne l'application de toute mesure visant à protéger les droits des personnes concernées.

Si l'incident de confidentialité présente un risque de préjudice sérieux, la CAI peut également ordonner à la FADQ d'aviser les personnes concernées si celle-ci ne l'a pas fait alors qu'elle était tenue de le faire.

La CAI peut également ordonner la remise des renseignements personnels à la FADQ, de même que leur destruction.

H. Modalités de traitement d'un incident de confidentialité

Il est à noter que les modalités de traitement d'un incident de confidentialité peuvent être réalisées simultanément. Afin d'illustrer les modalités, un schéma sur le traitement d'un incident de confidentialité impliquant un renseignement personnel est disponible à l'Annexe 1.

Titre : Directive sur les incidents de confidentialité impliquant des renseignements personnels

Code : 1132-14-00

Page 4 de 9

Émis le 2023-05-01

**Remplace
l'émission du :**

**Prochaine
révision :** 2026-05-01

1. Signaler l'incident de confidentialité ou la suspicion

Toute personne visée par la présente Directive qui a un motif de croire qu'il s'est produit un incident de confidentialité doit le signaler sans délai au RPRP en plus d'aviser le gestionnaire de l'unité visée.

Le signalement peut être fait de l'une des manières suivantes :

- par courriel à l'adresse suivante : sg_acces_plaintes@fadq.qc.ca
- ou directement auprès du RPRP aux coordonnées suivantes :

M^{me} Isabelle Chabot
1400, boul. Guillaume-Couture, 4^e étage
Lévis (Québec) G6W 8K7
Téléphone : 418 838-5606, poste 6066
Télécopieur : 418 834-2238

L'Annexe 2 propose un formulaire de déclaration d'incident pouvant être utilisé aux fins du signalement.

2. Déterminer s'il s'agit d'un incident de confidentialité

En collaboration avec la personne qui a fait le signalement et le gestionnaire de l'unité visée, le RPRP détermine s'il s'agit d'un incident de confidentialité en identifiant :

- les circonstances de l'incident;
- les renseignements personnels impliqués;
- les personnes concernées;
- le problème, que ce soit une erreur, une vulnérabilité, etc.

Dans l'éventualité où il s'agit d'un incident de sécurité qui n'implique pas de renseignements personnels, c'est le Processus de gestion des incidents de sécurité de l'information qui trouve application.

Cette évaluation doit se poursuivre tant que tous les éléments n'ont pas été identifiés.

3. Déterminer la nature du préjudice

Le gestionnaire de l'unité visée en collaboration avec le RPRP doit effectuer l'évaluation de la gravité du risque de préjudice sur les personnes concernées, lorsqu'il s'agit d'un incident de confidentialité imputable à la FADQ. Pour ce faire, les éléments suivants sont considérés :

- la sensibilité des renseignements concernés;
- les conséquences appréhendées de leur utilisation;
- la probabilité qu'ils soient utilisés à des fins préjudiciables.

Le Responsable de la sécurité de l'information et le Responsable de l'éthique de la FADQ ainsi que des experts externes peuvent être impliqués.

Les conclusions de l'évaluation déterminent si les personnes concernées encourrent ou non un risque plausible de préjudice sérieux.

Dans le cas contraire, elle doit tout de même poursuivre ses travaux pour réduire les risques et éviter qu'un incident de même nature se produise à nouveau dans le futur.

4. Aviser lors d'un risque de préjudice sérieux

En présence d'un risque plausible de préjudice sérieux, la FADQ informe de l'incident de confidentialité les personnes et les entités suivantes :

- **La personne concernée**

Le gestionnaire de l'unité visée en collaboration avec le RPRP notifie un avis à la personne concernée. Cet avis se fait par tout moyen adéquat (exemples : courriel ou lettre postale). Les éléments suivants doivent être mentionnés dans l'avis :

- La description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison qui justifie l'impossibilité de la fournir;
- Une brève description des circonstances de l'incident;
- La date ou la période où l'incident a eu lieu, ou encore l'approximation si cette dernière n'est pas connue;
- Une brève description des mesures que la FADQ a prises ou qu'elle entend prendre, à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé;
- Les mesures que la FADQ suggère à la personne concernée de prendre afin de diminuer le risque qu'un préjudice lui soit causé ou encore d'atténuer un tel préjudice;
- Les coordonnées des personnes-ressources qui permettront aux personnes concernées de se renseigner davantage relativement à l'incident.

Il est possible pour la FADQ d'aviser les personnes concernées en ayant recours à un avis public, lorsqu'une des situations suivantes se présente :

- Le fait de transmettre l'avis est susceptible de causer un préjudice accru à la personne concernée;
- Le fait de transmettre l'avis est susceptible de représenter une difficulté excessive pour la FADQ;
- La FADQ n'a pas les coordonnées de la personne concernée.

La FADQ peut également aviser les personnes concernées au moyen d'un avis public lorsque les circonstances requièrent d'agir rapidement pour diminuer le risque qu'un préjudice sérieux soit causé ou afin d'atténuer un tel préjudice. Dans ce cas, la FADQ demeure tenue de transmettre avec diligence un avis à la personne concernée. L'avis public peut être fait par tout moyen dont on peut raisonnablement s'attendre à ce qu'il permette de joindre la personne concernée.

La FADQ n'est pas tenue d'informer la personne concernée aussi longtemps que la transmission de cette information serait susceptible d'entraver une enquête menée par un organisme chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois. À partir du moment où le fait de l'informer n'est plus susceptible d'entraver une telle enquête, la FADQ doit rapidement aviser les personnes concernées.

Il est à noter qu'en l'absence d'un risque plausible de préjudice sérieux, la FADQ peut choisir d'informer la personne concernée pour des raisons de transparence ou de gestion des affaires. Ces raisons doivent être documentées dans le Registre des incidents de confidentialité.

- **La CAI**

Le RPRP transmet l'avis à la CAI à l'aide du formulaire¹ prévu à cet effet en suivant la procédure détaillée sur ledit formulaire.

¹ https://www.cai.gouv.qc.ca/documents/CAI_FO_avis_incident_confidentialite.pdf

Toute information complémentaire touchant les éléments que doit contenir l'avis à la CAI et dont la FADQ prend connaissance après l'envoi de cet avis doit être transmise, avec diligence.

- **Personne ou organisme susceptible de diminuer le préjudice**

Seuls les renseignements personnels, nécessaires à une personne ou un organisme susceptible de diminuer le préjudice, peuvent être communiqués sans le consentement de la personne concernée. Le RPRP inscrit la communication dans un Registre de communication.

- **Service de police compétent**

Dans l'éventualité où l'incident de confidentialité constitue un crime, la FADQ en informe le service de police compétent.

Les informations relatives aux avis à la CAI ainsi qu'aux personnes concernées sont documentées au Registre des incidents de confidentialité par le RPRP.

5. Poser des actions correctives et préventives

Le gestionnaire de l'unité visée par l'incident de confidentialité, le RPRP ainsi que, le cas échéant, le Responsable de la sécurité de l'information ou toute autre personne requise selon la situation :

- appliquent les mesures correctrices qui s'imposent afin de faire cesser l'incident de confidentialité;
- adoptent les mesures préventives qui leur paraissent appropriées afin d'éviter qu'un tel incident de confidentialité se reproduise.

Le RPRP collige au Registre des incidents de confidentialité une brève description des mesures prises par la FADQ afin de diminuer les risques qu'un préjudice soit causé.

I. Tenue d'un Registre des incidents de confidentialité

Le Registre des incidents de confidentialité permet de documenter tous les incidents de confidentialité survenus, même ceux ne présentant pas de risque de préjudice sérieux.

Ce registre permet de bonifier les plans de résilience, d'orienter au besoin l'offre de formation et de sensibilisation à la protection des renseignements personnels et d'améliorer en continu la gestion des incidents de confidentialité.

À la demande de la CAI, la FADQ doit lui transmettre une copie du Registre des incidents de confidentialité.

Le Registre des incidents de confidentialité répertorie notamment pour chaque incident les éléments suivants :

- 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;
- Une brève description des circonstances de l'incident;
- La date ou la période de survenance de l'incident ou, si cette dernière n'est pas connue, une approximation de cette période;
- La date ou la période de la prise de connaissance de l'incident par la FADQ;
- Le nombre de personnes concernées par l'incident;
- Une description des éléments qui amènent la FADQ à conclure qu'il existe ou non un risque qu'un préjudice sérieux soit causé aux personnes concernées, telle 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;

Titre : Directive sur les incidents de confidentialité impliquant des renseignements personnels

Code : 1132-14-00

Page 7 de 9

Émis le 2023-05-01

**Remplace
l'émission du :**

**Prochaine
révision :** 2026-05-01

- La description des mesures prises par la FADQ pour remédier, atténuer ou contenir les conséquences négatives de l'incident de confidentialité et celles pour éviter qu'un tel incident se reproduise;
- Les dates et moyens des notifications de l'incident de confidentialité ainsi que les motifs de notification aux personnes concernées en l'absence d'un risque plausible de préjudice sérieux.

Les renseignements contenus au Registre des incidents de confidentialité doivent être tenus à jour et conservés pendant une période minimale de cinq ans après la date ou la période au cours de laquelle la FADQ a pris connaissance de l'incident.

J. Révision de la Directive

La Directive fera l'objet d'une révision tous les trois ans par le RPRP, sauf s'il est nécessaire de le faire avant.

K. Diffusion de la Directive

Le RPRP est responsable de la diffusion de la Directive au sein de la FADQ et de son application.

L. Approbation et entrée en vigueur

Cette directive a été approuvée par le président-directeur général et prend effet à la même date.

Ernest Desrosiers
ERNEST DESROSIERS
Président-directeur général

1^{er} mai 2023
Date d'approbation



Annexe 1

Processus de traitement d'un incident de confidentialité (Section H)

1. Signaler l'incident de confidentialité

Motif de croire que s'est produit un incident de confidentialité

Employé ou tiers: Signale sans délai au RPRP et en avise son gestionnaire.

2. Déterminer s'il s'agit d'un incident de confidentialité

Personne qui a fait le signalement, gestionnaire de l'unité visée et RPRP: Détermine les circonstances de l'incident, les renseignements personnels impliqués, les personnes concernées et le problème.

3. Déterminer la nature du préjudice

Gestionnaire de l'unité visée en collaboration avec le RPRP (le Responsable de la sécurité de l'information et le Responsable de l'éthique de la FADQ ainsi que des experts externes peuvent être impliqués) : Effectue l'évaluation de la gravité du risque de préjudice sur les personnes concernées (sensibilité du renseignement personnel, conséquences appréhendées et probabilité d'utilisation à des fins préjudiciables).

4. Aviser lors d'un risque de préjudice sérieux

Gestionnaire de l'unité visée en collaboration avec le RPRP : Informe les personnes concernées ainsi que les personnes ou entités requises par la situation. Le RPRP avise la CAI.

5. Poser des actions correctives et préventives

Gestionnaire de l'unité visée en collaboration avec le RPRP (le cas échéant le Responsable de la sécurité de l'information ou toute autre personne requis par la situation) : Applique des mesures correctrices et adopte des mesures préventives appropriées pour faire cesser l'incident de confidentialité et éviter qu'il ne se reproduise.

RPRP : Documente l'incident de confidentialité au Registre des incidents de confidentialité.

Annexe 2

FORMULAIRE DE SIGNALEMENT D'UN INCIDENT DE CONFIDENTIALITÉ

IDENTIFICATION DU SIGNALANT		
Nom	Prénom	
Unité administrative		
Centre de responsabilité (C.R.)		
NATURE DE L'INCIDENT (cochez la bonne case)		
<input type="checkbox"/> Vol ou sabotage d'un équipement	<input type="checkbox"/> Intrusion technique (pirate informatique)	
<input type="checkbox"/> Virus ou canulars	<input type="checkbox"/> Autres	
<input type="checkbox"/> Intrusion physique (utilisation illégale du mot de passe, usurpation d'identité, indiscretion dans un ordinateur)		
INCIDENT		
Date ou période de l'incident	Début de la prise en charge	Fin des interventions
Description des circonstances de l'incident		
Description des renseignements personnels visés par l'incident		
Description des personnes concernées et le nombre		
Actif informationnel impliqué (équipements informatiques, système d'information et banque de données)		
DÉTENTEUR DE L'ACTIF		
Nom	Prénom	
Localisation (adresse complète)		
DÉTAILS DE L'INTERVENTION		
Prise en charge du signalement		
Mesures correctives et préventives		

2023-04-25

Vous pouvez transmettre le Formulaire de signalement d'un incident de confidentialité à l'adresse courriel suivante : sg_acces_plaintes@fadq.qc.ca