

Directive concernant le traitement d'un incident de confidentialité impliquant des renseignements personnels

Instance : Comité de régie

	Date	Résolution
Adoption	12 décembre 2022	N/A
Modifications		

Prochaine révision Décembre 2025

Responsable Secrétariat général

**Directive concernant le traitement d'un incident de confidentialité
impliquant des renseignements personnels**

Table des matières

1	Énoncé de principe	3
2	Objectif (s)	3
3	Champ d'application	3
4	Cadre juridique	3
5	Définition (s)	3
6	Rôles et responsabilités	4
7	Dispositions générales	6
7.1	Limitation des conséquences	6
7.1.1	Mesures à mettre en place	6
7.1.2	Évaluation de l'incident de confidentialité	7
8	Responsable de l'application et de la mise à jour	7
9	Adoption et entrée en vigueur	7
Annexe 1		8
	Registre des incidents de confidentialité	8

Directive concernant le traitement d'un incident de confidentialité impliquant des renseignements personnels

1 Énoncé de principe

L'Université du Québec entend mettre en place les mesures nécessaires pour se conformer à ses obligations légales et être prête à agir en cas d'incident de confidentialité.

2 Objectif (s)

La directive a pour objectif d'assurer une gestion efficace de tout incident de confidentialité relatif aux renseignements personnels par la définition des rôles et des responsabilités des intervenants concernés par cet incident et par l'Université du Québec, le cas échéant, d'une stratégie d'intervention propre à corriger la situation y ayant conduit.

Elle vise donc à mettre en place des mesures immédiates et préventives permettant de limiter les conséquences découlant d'un tel incident et d'éviter que l'incident de confidentialité constaté ne se produise à nouveau. Elle établit en outre les modalités permettant d'aviser la personne concernée par l'incident de confidentialité relatif à des renseignements personnels.

3 Champ d'application

La directive s'applique à tout incident de confidentialité, qu'il soit intentionnel ou accidentel, découlant du fait de tout.e dirigeant.e, employé.e ou mandataire de l'Université du Québec, ci-après « UQ ».

4 Cadre juridique

La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ chapitre A-2.1), ci-après « loi »;

Code civil du Québec (RLRQ chapitre C-1991);

Politique sur la sécurité et la gestion des ressources informationnelles de l'Université du Québec.

5 Définition (s)

Pour l'application de la directive, on entend par :

- Incident de confidentialité (cf. Article 63.9 de la loi)
 - L'accès non autorisé par la loi, à un renseignement personnel.

Directive concernant le traitement d'un incident de confidentialité impliquant des renseignements personnels

- L'utilisation d'un renseignement personnel à des fins autres que celles prévues par la loi.
 - 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
- Mandataire de l'UQ
Toute personne qui exécute un mandat pour l'UQ tels un consultant, un.e prestataire de service ou un.e employé.e en prêt de service.
 - Renseignement personnel
Tout renseignement qui concerne une personne physique et qui permet de l'identifier.
 - Sécurité de l'information
Ensemble des moyens technologiques, humains, organisationnels, juridiques et éthiques permettant d'assurer la réalisation des objectifs de disponibilité, d'intégrité et de confidentialité de l'information.

6 Rôles et responsabilités

- Employé.e ou mandataire
Tout.e employé.e ou mandataire de l'UQ qui constate un incident de confidentialité doit le signaler sans délai à son supérieur.e.
- Supérieur.e
Tout.e gestionnaire ou personne en autorité à l'UQ, qui est informé ou a connaissance de l'existence d'un incident de confidentialité, doit le signaler sans délai au responsable ou à la responsable de l'accès aux documents et de la protection des renseignements personnels de l'UQ.
- Responsable de l'accès aux documents et de la protection des renseignements personnels
Le secrétaire général ou la secrétaire générale est le ou la responsable de l'accès aux documents et de la protection des renseignements personnels (RAPRP).
Le ou la RAPRP informe le président ou la présidente et le vice-président ou la vice-présidente duquel relève l'unité administrative concernée par l'incident de confidentialité.
Le ou la RAPRP soutient le gestionnaire ou la gestionnaire du secteur concerné par l'incident de confidentialité, notamment dans la mise en place de mesures immédiates et préventives pour limiter les conséquences découlant d'un tel

Directive concernant le traitement d'un incident de confidentialité impliquant des renseignements personnels

incident et de toutes autres mesures qui pourraient être jugées nécessaires, ou pour éviter que l'incident de confidentialité constaté ne se produise à nouveau ou perdure.

Le ou la RAPRP procède à l'analyse de l'évaluation de la situation ayant conduit à l'incident de confidentialité produite par le ou la gestionnaire de l'unité administrative concernée et soumet ses recommandations au président ou à la présidente accompagnées, le cas échéant, de l'avis du vice-président ou de la vice-présidente concerné.e ou celui du Comité sur l'accès à l'information et sur la protection des renseignements personnels (CAIPRP), sur les mesures qu'il recommande.

Le ou la RAPRP tient à jour un registre sur les situations impliquant un incident de confidentialité relatif aux renseignements personnels et le dépose au CAIPRP (cf. Article 63.11 de la Loi).

- Gestionnaire de l'unité administrative concernée par l'incident de confidentialité

Le ou la gestionnaire de l'unité administrative concernée par l'incident de confidentialité procède à l'évaluation de la situation en colligeant toutes les informations pertinentes à cette fin. Il ou elle indique, le cas échéant, les mesures immédiates à mettre en place pour limiter les conséquences découlant d'un tel incident et les autres mesures visant notamment à éviter que l'incident de confidentialité constaté ne se produise à nouveau ou perdure. Il ou elle transmet cette évaluation, accompagnée de ses recommandations, au RAPRP, en y incluant les mesures immédiates ainsi que les autres mesures qui pourraient être jugées nécessaires.

Après consultation du ou de la RAPRP, il ou elle met en place les mesures immédiates et toutes autres mesures qui pourraient s'avérer nécessaires pour l'avenir tel que décider par le président ou la présidente et il ou elle avise le ou la RAPRP lorsque l'opération est complétée.

- Vice-président

Le vice-président ou la vice-présidente duquel.le relève l'unité administrative concernée par l'incident de confidentialité s'assure que le ou la gestionnaire de cette unité effectue son évaluation dans les meilleurs délais. De plus, il formule son avis au RAPRP en regard de la mise en place des mesures recommandées visant à éviter que l'incident de confidentialité constaté ne se produise à nouveau ou perdure. Enfin, il s'assure que les mesures décidées par le président ou la présidente sont mises en place promptement.

- Président

Directive concernant le traitement d'un incident de confidentialité impliquant des renseignements personnels

Le président ou la présidente statue, après avoir pris connaissance de l'analyse du ou de la RAPRP et de l'avis du vice-président ou de la vice-présidente duquel. Le relève l'unité administrative concernée par l'incident de confidentialité ainsi que, le cas échéant, celui du ou de la RAPRP, sur les mesures à mettre en place visant à éviter que l'incident de confidentialité constaté ne se produise à nouveau ou perdure. En outre, il approuve la directive et toute modification ultérieure à celle-ci.

7 Dispositions générales

7.1 Limitation des conséquences

Dès qu'il ou elle constate l'existence d'un incident de confidentialité, le secrétaire général ou la secrétaire générale prend promptement les mesures raisonnables pour limiter les conséquences et pour éviter qu'un incident de confidentialité se produise à nouveau. Ainsi, dès qu'il ou elle en est informé.e, le ou la gestionnaire de l'unité administrative concernée par l'incident met en place des mesures immédiates et préventives et procède, par la suite, à l'évaluation de l'incident de confidentialité ainsi que des mesures déjà déployées et les autres qui devraient l'être.

7.1.1 Mesures à mettre en place

Dans le but de limiter les conséquences liées à l'incident de confidentialité, certaines mesures doivent, le cas échéant, être mises en place le plus rapidement possible, à savoir notamment :

- Avis par le ou la RAPRP à la personne concernée par le renseignement personnel faisant l'objet d'un incident de confidentialité;
- Contact auprès de la personne qui a eu accès à un renseignement personnel auquel elle n'avait pas le droit d'avoir accès par le ou la RAPRP et signature d'un engagement de confidentialité par la personne qui a eu accès à ce renseignement personnel;
- Cessation immédiate de la pratique ayant conduit à l'incident de confidentialité;
- Modification, voire révocation, par le ou la gestionnaire de l'unité administrative concernée, lorsque requis, d'un mot de passe ou d'un code d'accès, en application de la Politique sur la sécurité et la gestion des ressources informationnelles;
- Modification, par le ou la responsable de la sécurité de l'information de l'UQ, aux systèmes informatiques impliqués dans l'incident de confidentialité;
- Avis par le ou la RAPRP, lorsque le renseignement personnel ayant fait l'objet de l'incident de confidentialité est détenu pour le compte d'un organisme public (établissements ou clientèle de l'UQ), à l'organisme concerné.

Directive concernant le traitement d'un incident de confidentialité impliquant des renseignements personnels

7.1.2 Évaluation de l'incident de confidentialité

L'évaluation de l'incident de confidentialité doit mener à une ou des recommandations et se faire notamment en :

- Identifiant précisément les renseignements personnels concernés;
- Déterminant leur degré de sensibilité;
- Procédant à une analyse détaillée de la chronologie des actes, des interventions, des ordres ou des omissions ayant conduit à l'incident de confidentialité;
- Évaluant les conséquences causées et en identifiant celles qui pourraient ultérieurement découler à l'incident de confidentialité;
- Évaluant les impacts possibles sur la mission de l'UQ;
- Considérant notamment la sensibilité du renseignement personnel concerné, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables (cf. Article 63.8 de la Loi);
- Déterminant si les mesures mises en place conformément à la section 7.1.1 sont suffisantes pour éviter que l'incident de confidentialité ou qu'un incident de même nature se produise à nouveau ou perdure et si d'autres mesures doivent être appliquées (par exemple : modification aux systèmes informatiques, acquisition de solutions de protection, octroi de mandats de services professionnels, etc.);
- Déterminant si une intervention en matière de communication est requise et, le cas échéant, en déterminer l'ampleur (au niveau des personnes concernées de la direction visée, voire à l'ensemble du personnel de l'UQ);
- Déterminant, compte tenu de la nature des actes, des interventions, des ordres ou des omissions ayant conduit à l'incident de confidentialité, s'il y a lieu de dénoncer ceux-ci à un corps de police ou à tout organisme qui, en vertu de la loi, est chargé de prévenir, de détecter ou de réprimer le crime ou une infraction à une loi applicable au Québec.

8 Responsable de l'application et de la mise à jour

Le secrétaire général ou la secrétaire générale est responsable de l'application de la présente directive, laquelle est révisée au besoin ou mise à jour tous les trois ans.

9 Adoption et entrée en vigueur

Cette directive est entrée en vigueur le 12 décembre 2022, date de son adoption par le comité de régie.

Registre des incidents de confidentialité

En vertu de l'article 63.11¹ de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1) telle que modifiée par la [Loi sur la modernisation de certaines dispositions législatives en matière de protection des renseignements personnels](#) (LQ 2021, c. 25), un organisme public, incluant une université, doit tenir un registre des incidents de confidentialité. Ce registre doit être transmis, sur demande, à la Commission d'accès à l'information.

Le registre des incidents de confidentialité doit contenir les éléments ci-dessous. Ces éléments doivent être tenus à jour et conservés pendant une période minimale de cinq (5) ans après la date ou la période au cours de laquelle l'entreprise a pris connaissance de l'incident.

Registre des incidents de confidentialité									
	Description des renseignements personnels visés par l'incident Note – si cette information n'est pas connue, indiquer la raison justifiant l'impossibilité de fournir une telle description	Description des circonstances de l'incident Note : accès, utilisation, communication non autorisé(e), perte ou autre atteinte à la protection des renseignements personnels	Date ou période de l'incident Note – si cette période n'est pas connue, indiquer une approximation de cette période	Date ou période de la prise de connaissance de l'incident	Nombre de personnes concernées par l'incident Note – si ce nombre n'est pas connu, indiquer une approximation de celui-ci	Description des éléments qui amènent à conclure qu'il existe ou non un risque qu'un préjudice sérieux soit causé aux personnes concernées Note – sensibilité des renseignements personnels/utilisations malveillantes possibles de ceux-ci/conséquences appréhendées de leur utilisation/probabilité qu'ils soient utilisés à des fins préjudiciables	Date de transmission de l'avis à la Commission d'accès à l'information ²	Date de transmission des avis aux personnes concernées Note – si des avis publics ont été émis pour rejoindre les personnes concernées, indiquer la date et la raison de ces avis publics	Description des mesures prises afin de diminuer les risques qu'un préjudice soit causé
1.									
2.									

¹ Date d'entrée en vigueur : 22 septembre 2022.

² [Formulaire de déclaration](#) à la CAI.