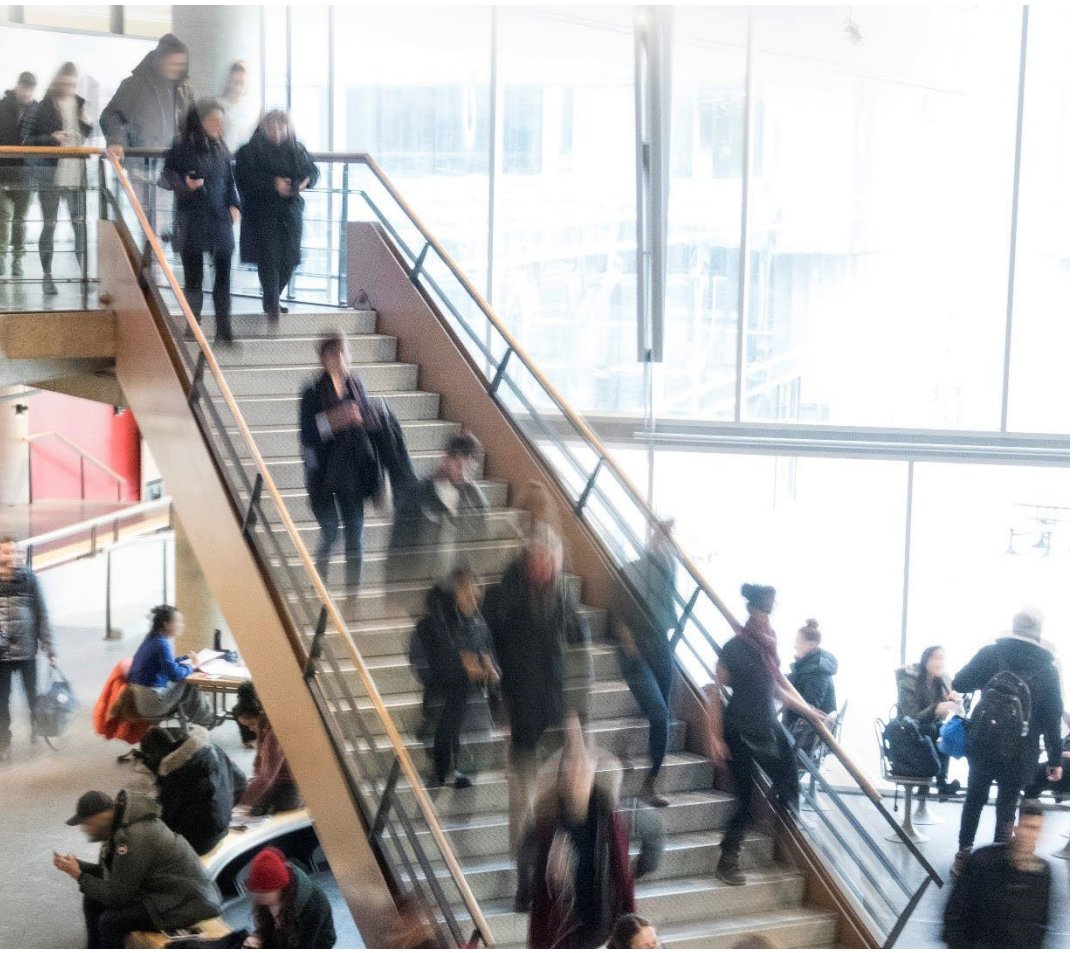
UQÀM | Université du Québec à Montréal



# Procédure sur la gestion des incidents de confidentialité impliquant des renseignements personnels

**Dernière mise à jour**
**29 août 2023**

| | |
|---|---|
| Responsable de l'application | Secrétaire générale, secrétaire général |
| Autorité compétente | Comité sur l'accès à l'information et la protection des renseignements personnels |
| Signature | Marylène Drouin UQÀM<br>Signé avec ConsignO Cloud (20/12/2023)<br>Vérifiez avec verifio.com ou Adobe Reader. |
| Date d'approbation | 29 août 2023 |
| Date d'entrée en vigueur | 29 août 2023 |
| Date de la dernière modification | |

# Table des matières

# 1. Préambule

Tel que le prévoient les règles de gouvernance établies dans la Directive sur le traitement et la protection des renseignements personnels, l'Université du Québec à Montréal (ci-après, l'« Université ») reconnaît l'importance de protéger les renseignements personnels qu'elle détient, peu importe leur support, et traite de façon générale des règles liées aux incidents de confidentialité.

Plus précisément et afin de se conformer aux obligations prévues à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, l'Université se dote de cette procédure pour gérer d'éventuels incidents de confidentialité.

Bien que l'Université mette en place des mesures de sécurité raisonnables pour protéger les renseignements personnels qu'elle traite, peu importe leur support, il est possible qu'un incident de confidentialité survienne.

Généralement, la gestion d'un incident de confidentialité s'inscrit dans le processus plus large de gestion des incidents de sécurité de l'information. Les incidents de sécurité ne visent pas toujours des renseignements personnels. Au sens de la présente procédure, les incidents de confidentialité impliquent nécessairement des renseignements personnels.

# 2. Objet

Cette procédure encadre la gestion des incidents de confidentialité qui sont portés à la connaissance de l'Université, notamment en décrivant les étapes à suivre lorsqu'une personne détecte un incident de confidentialité et les rôles et responsabilités des parties prenantes.

# 3. Champ d'application

La Procédure sur la gestion des incidents de confidentialité impliquant des renseignements personnels s'applique à tout incident de confidentialité impliquant des renseignements personnels détenus par l'Université, détecté par toute personne, membre du personnel ou non de l'Université.

Cette procédure s'applique également à tout incident de sécurité affectant négativement la sécurité d'un ou plusieurs actifs informationnels, lorsqu'un tel incident concerne des renseignements personnels détenus par l'Université.

Elle s'applique également aux incidents de confidentialité impliquant des renseignements personnels confiés par l'Université dans le cadre de l'exécution d'un mandat ou d'un contrat de service.

# 4. Cadre juridique

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

- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ c. A -2.1 (ci-après, la « Loi sur l'accès ») et ses règlements, dont le Règlement sur les incidents de confidentialité, RLRQ c. A-2.1, r. 3.1 ;
- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, RLRQ c. G-1.03;
- Règlement sur les modalités et conditions d'application des articles 12.2 à 12.4 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, RLRQ c. G-1.03, r. 1;
- Loi concernant le cadre juridique des technologies de l'information, RLRQ c. C-1.1;
- Directive sur le traitement et la protection des renseignements personnels.

# 5. Définitions

Aux fins de cette procédure, les termes suivants se définissent comme suit :

a) événement de sécurité : indication que la sécurité (confidentialité, intégrité, disponibilité) d'un ou de plusieurs actifs informationnels ait pu ou pourrait éventuellement être affectée;

b) gestionnaire : cadre supérieure, cadre supérieur, cadre, doyenne, doyen. En ce qui concerne le personnel enseignant, la, le gestionnaire, au sens de cette procédure, est la vice-rectrice, le vice-recteur à la Vie académique;

c) incident de confidentialité : l'accès, l'utilisation ou la communication d'un renseignement personnel non autorisé par la Loi sur l'accès, ainsi que la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement;

d) incident de sécurité : un ou plusieurs événements de sécurité (confidentialité, intégrité, disponibilité) confirmés et affectant négativement la sécurité d'un ou plusieurs actifs informationnels;

e) membres du personnel : toute personne à l'emploi de l'Université et qui en reçoit un traitement ou un salaire, qu'elle soit permanente, régulière ou occasionnelle, ainsi que toute personne désignée comme professeure associée, professeur associé ou professeure visiteuse, professeur visiteur;

f) personne concernée : personne physique dont un ou plusieurs renseignements personnels la concernant sont visés par un incident de confidentialité;

g) renseignement personnel : tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier. Le fait qu'une signature apparaisse au bas d'un document n'a pas pour effet de rendre personnels les renseignements qui y apparaissent. Aux fins de cette procédure, cette définition correspond à « renseignements personnels » au sens où l'entend la Loi sur l'accès, la Loi sur la protection des renseignements personnels dans le secteur privé (« LPRSP ») et, lorsque applicables, la Loi sur la protection des renseignements personnels et les documents électroniques (« LRPDE »), et est équivalente à celle des « données à

caractère personnel » au sens ou l'entend le Règlement général sur la protection des données (« RGPD »);

h) renseignement sensible : renseignement personnel qui, du fait de 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;

i) responsable de la protection des renseignements personnels : la secrétaire générale, le secrétaire général, est la, le responsable de la protection des renseignements personnels, tel que délégué par écrit par la rectrice, le recteur en vertu de l'article 8 de la Loi sur l'accès. La directrice exécutive, le directeur exécutif du Secrétariat général agit à titre de responsable substitut, le cas échéant, tel que délégué par écrit par la rectrice, le recteur en vertu de l'article 8 de la Loi sur l'accès.

# 6. Processus de traitement d'un incident de confidentialité

## 6.1 Signalement

### 6.1.1 Signalement par un membre du personnel

Tout membre du personnel qui détecte ou suspecte un incident de confidentialité ou qui en est informé signale sans délai cet incident de confidentialité en remplissant le formulaire de signalement disponible sur le site web des Services informatiques de l'Université.

Cette personne informe également sa, son gestionnaire de ce signalement.

Le formulaire est ainsi reçu par la direction des Services informatiques de l'Université, laquelle assure les suivis auprès de la, du membre du personnel et de sa, son gestionnaire et de toute autre personne, au besoin.

### 6.1.2 Signalement par une personne étudiante

Toute personne étudiante qui détecte ou suspecte un incident de confidentialité ou qui en est informée signale sans délai cet incident de confidentialité en remplissant un formulaire de signalement disponible sur le site web des Services informatiques de l'Université.

Le formulaire est ainsi reçu par la direction des Services informatiques de l'Université, laquelle assure les suivis auprès de la personne étudiante et de toute autre personne, au besoin.

### 6.1.3 Signalement par toute autre personne

Toute autre personne signale sans délai l'incident de confidentialité à la, au responsable de la protection des renseignements personnels par courriel à l'adresse suivante : accesinformation@uqam.ca.

La, le responsable remplit ensuite sans délai le formulaire de signalement disponible sur le site web des Services informatiques de l'Université.

Le formulaire est ainsi reçu par la direction des Services informatiques de l'Université, laquelle assure les suivis auprès de la, du responsable de la protection des renseignements personnels et de toute autre personne, au besoin.

## 6.2 Diminution du risque et contention

Lorsque cela est possible, la personne ayant signalé l'incident de confidentialité doit mettre en place sans délai des mesures raisonnables afin de contenir l'incident et diminuer les risques qu'un préjudice soit causé aux personnes concernées. Cette étape s'exerce en collaboration avec les Services informatiques de l'Université.

## 6.3 Analyse et évaluation

Les Services informatiques de l'Université prennent connaissance du formulaire de signalement et vérifient qu'il s'agit bien d'un incident de confidentialité, et le cas échéant, d'un incident de sécurité. Cette vérification doit :

a) établir les circonstances de l'incident;
b) identifier les renseignements personnels impliqués;
c) identifier les personnes concernées;
d) identifier la cause et l'étendue de l'incident.

Dans le cas d'un incident de confidentialité confirmé, les Services informatiques de l'Université informent la, le responsable de la protection des renseignements personnels et évaluent les préjudices prévisibles pour les personnes concernées, après consultation de la, du responsable de la protection des renseignements personnels.

Dans le cadre de cette évaluation, les Services informatiques prennent notamment en compte les éléments suivants :

a) la sensibilité des renseignements personnels visés;

b) les conséquences appréhendées de l'utilisation des renseignements personnels;

c) la probabilité qu'ils soient utilisés à des fins préjudiciables.

Dans le cas d'un incident de confidentialité susceptible de causer un préjudice sérieux aux personnes concernées par les renseignements personnels, les Services informatiques forment une équipe de gestion de l'incident, en collaboration avec la, le responsable de la sécurité de l'information et la, le responsable de la protection des renseignements personnels. La rectrice, le recteur en est également informée, informé.

## 6.4 Mesures correctives

Les Services informatiques et, dans le cas d'un risque de préjudice sérieux, la, le responsable de la protection des renseignements personnels prennent les mesures appropriées ou fournissent aux gestionnaires des unités concernées par l'incident de confidentialité des conseils et instructions concernant les mesures correctives à mettre en place afin de limiter l'atteinte et d'éviter que de nouveaux incidents de même nature ne se produisent.

Les gestionnaires collaborent à la mise en place des mesures identifiées.

Les mesures mises en place sont consignées au formulaire de signalement.

## 6.5 Notification de l'incident de confidentialité en présence d'un risque de préjudice sérieux

### 6.5.1 Avis à la personne concernée

Lorsqu'il a été déterminé qu'un incident de confidentialité présente un risque de préjudice sérieux, le gestionnaire de l'unité doit aviser la personne concernée, en collaboration avec les Services informatiques, le cas échéant. Cet avis doit comprendre :

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 l'Université a prises ou entend prendre à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé;

e) les mesures que l'Université suggère à la personne concernée de prendre afin de diminuer le risque qu'un préjudice lui soit causé afin d'atténuer un tel préjudice;

f) les coordonnées permettant à la personne concernée de se renseigner davantage relativement à l'incident.

L'avis à la personne concernée peut être donné au moyen d'un avis public dans l'une ou l'autre circonstance suivante :

a) lorsque le fait de transmettre l'avis est susceptible de causer un préjudice accru à la personne concernée;

b) lorsque le fait de transmettre l'avis est susceptible de représenter une difficulté excessive pour l'Université;

c) lorsque l'Université n'a pas les coordonnées de la personne concernée.

Malgré ce qui précède, l'Université n'a pas à aviser la personne concernée 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, de détecter ou de réprimer le crime ou les infractions aux lois.

### 6.5.2 Avis à la Commission d'accès à l'information

Lorsqu'il a été déterminé qu'un incident de confidentialité présente un risque sérieux de préjudice, la, le responsable de la protection des renseignements personnels doit aviser la Commission d'accès à l'information. L'avis doit contenir l'information prescrite par le formulaire de déclaration de la Commission d'accès à l'information disponible sur le site Web de cette dernière.

### 6.5.3 Avis à d'autres autorités

Dans certains cas particuliers ou dans le cas d'un incident de confidentialité constituant également un incident de sécurité, l'Université avise d'autres autorités, si nécessaire.

En cas de doute de la commission d'une infraction criminelle, le Service de prévention et de sécurité de l'Université est informé par les Services informatiques et effectue les suivis auprès des autorités policières.

## 6.6 Notification de l'incident de confidentialité en l'absence d'un risque de préjudice sérieux

Le gestionnaire de l'unité, en collaboration avec les Services informatiques, le cas échéant, détermine s'il est pertinent d'informer la personne concernée.

# 7. Registre des incidents de confidentialité

L'Université tient un registre des incidents de confidentialité, lequel est sous la responsabilité de la, du responsable de la protection des renseignements personnels. Le registre contient les éléments suivants concernant tout incident de confidentialité :

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) la date ou la période au cours de laquelle l'Université a pris connaissance de l'incident;

e) le nombre de personnes concernées par l'incident ou, s'il n'est pas connu, une approximation de ce nombre;

f) une description des éléments qui amènent l'Université à conclure qu'il existe ou non un risque qu'un préjudice sérieux soit causé aux personnes concernées;

g) si l'incident présente un risque qu'un préjudice sérieux soit causé : les dates de transmission des avis à la Commission d'accès à l'information et aux personnes concernées, de même qu'une mention indiquant si des avis publics ont été donnés par l'Université et la raison pour laquelle ils l'ont été, le cas échéant;

h) une brève description des mesures prises par l'Université, à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé.

## 8. Bilan et mesures préventives

Lorsque les étapes précédentes sont réalisées, les Services informatiques et la, le gestionnaire concerné effectuent un bilan de l'incident et déterminent, le cas échéant, les mesures à adopter afin de prévenir les incidents ultérieurs de même nature.

Dans le cas d'un incident de confidentialité susceptible de causer un préjudice sérieux aux personnes concernées par les renseignements personnels, les Services informatiques réalisent cette étape en collaboration avec l'équipe de gestion de l'incident.

## 9. Responsable de l'application

La, le responsable de la protection des renseignements personnels, soit la secrétaire générale, le secrétaire général est responsable de l'application de cette procédure.

## 10. Entrée en vigueur

Cette procédure entre en vigueur au moment de son adoption par l'autorité compétente.

## 11. Mise à jour

Cette procédure est mise à jour minimalement tous les cinq ans.