BIBLIOTHÈQUE NATIONALE
ARCHIVES NATIONALES
GRANDE BIBLIOTHÈQUE

DIRECTIVE RELATIVE À LA GESTION DES INCIDENTS DE CONFIDENTIALITÉ (D-5)

Adoptée par le conseil de direction le 26 septembre 2022

DIRECTIVE RELATIVE À LA GESTION DES INCIDENTS DE CONFIDENTIALITÉ

Adoption :	
Conseil de direction	26 septembre 2022

Table des matières

DIRECTIVE RELATIVE À LA GESTION DES INCIDENTS DE CONFIDENTIALITÉ

PRÉAMBULE

La présente directive met en place à Bibliothèque et Archives nationales du Québec (« **BAnQ** ») un cadre de gestion des incidents de confidentialité conforme aux nouvelles obligations en matière de protection des renseignements personnels qui entrent en vigueur le 22 septembre 2022, suivant l'adoption et la sanction de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*.

1. DÉFINITIONS

À moins de mention contraire ou que le contexte n'indique un sens différent, les définitions de l'article 1 de la Directive encadrant le corpus règlementaire (D-1) s'appliquent à la présente directive.

De plus, dans le cadre de l'application de la présente directive, on entend par :

a) **« COMITÉ AIPRP » :** comité sur l'accès à l'information et sur la protection des renseignements personnels;

b) **« COMITÉ SI » :** comité sur la sécurité de l'information, dont la composition et le mandat sont prévus dans la Politique en matière de sécurité de l'information de BAnQ (P-3);

c) **« COMMISSION » :** Commission d'accès à l'information du Québec;

d) **« CRISE » :** situation de crise telle que définie dans le Plan de gestion de crise de BAnQ;

e) **« INCIDENT DE CONFIDENTIALITÉ » :** tout incident qui correspond à l'une ou l'autre des situations suivantes :

i. l'accès non autorisé par la loi à un renseignement personnel;

ii. l'utilisation non autorisée par la loi d'un renseignement personnel;

iii. la communication non autorisée par la loi d'un renseignement personnel;

iv. la perte d'un renseignement personnel ou toute atteinte à la protection d'un tel renseignement;

f) **« PDG » :** président-directeur général;

g) **« RENSEIGNEMENT PERSONNEL » :** tout renseignement qui concerne une personne physique et permet de l'identifier;

h) **« RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS » OU « RESPONSABLE PRP » :** le pdg ou la personne désignée par celui-ci conformément à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*;

2. OBJECTIFS

La présente directive vise à :

- mettre en place un cadre de gestion des incidents de confidentialité;

- établir la procédure à suivre en cas d'incident;
- préciser les responsabilités des intervenants en cas d'incident;
- déterminer les modalités de la tenue d'un registre des incidents et des déclarations obligatoires requises en cas d'incident.

3. CHAMP D'APPLICATION

La présente directive s'applique à tous les membres du personnel et à toutes les unités administratives de BAnQ.

4. CADRE JURIDIQUE

Le cadre juridique de la présente directive est notamment composé des lois et règlements suivants :

a) la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels,* RLRQ, c. A-2.1 (« **Loi sur l'accès** »);

b) la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, RLRQ, c. 25;

c) le *Règlement sur les incidents de confidentialité.*

Il est complété par les éléments suivants du corpus règlementaire :

a) la Politique en matière de sécurité de l'information (P-3);

b) la Politique de gestion de l'information (P-4);

c) la Politique sur le partage et la valorisation des données institutionnelles (P-11);

d) la Politique de BAnQ en matière d'accès à l'information et de protection des renseignements personnels;

e) la Directive relative à la communication de renseignements personnels en vue d'assurer la protection des personnes;

f) la Directive relative à l'utilisation et à la communication de renseignements personnels à des fins d'étude, de recherche ou de production de statistiques;

g) la Procédure relative aux mesures de protection des renseignements personnels concernant les systèmes d'information ou de prestations électroniques de services, les sondages et la vidéosurveillance;

H) la Directive encadrant le corpus règlementaire (D-1).

5. DÉTECTION ET ÉVALUATION PRÉLIMINAIRE

Dès qu'une unité administrative a des motifs de croire que s'est produit un incident de confidentialité, l'annexe 1 doit être remplie et transmise au responsable PRP.

Le responsable PRP effectue une évaluation préliminaire de la situation. S'il détermine que cette dernière correspond à un incident de confidentialité, il transmet son évaluation préliminaire et l'annexe 1 aux membres du comité SI.

6. MESURES URGENTES POUR LIMITER L'ATTEINTE À LA VIE PRIVÉE

En cas d'incident de confidentialité, les unités administratives impliquées doivent prendre toute mesure urgente requise pour limiter les conséquences pour les personnes concernées, notamment la possibilité d'utilisation malveillante des renseignements personnels, l'usurpation ou le vol d'identité.

7. ÉVALUATION DU RISQUE ET MESURES À PRENDRE

En cas d'incident de confidentialité, le responsable PRP doit convoquer sans délai une séance du comité SI afin que celui-ci :

i. évalue le risque qu'un préjudice soit causé à une personne;

ii. détermine les mesures raisonnables devant être prises pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent.

Le comité SI doit se réunir aussi souvent que requis, selon la gravité de l'incident. Il peut convoquer tout membre du personnel jugé utile et doit documenter ses travaux, notamment en remplissant l'annexe 2.

8. PLAN DE GESTION DE CRISE

Si l'incident s'apparente à une crise, le responsable PRP doit communiquer avec le pdg afin que celui-ci décide s'il déclenche le plan de gestion de crise, auquel cas la cellule de crise prend le relais pour la gestion de l'incident.

9. DÉCLARATION DE L'INCIDENT

Le responsable PRP doit, avec diligence, aviser la Commission et les personnes concernées par les renseignements personnels si l'incident présente un risque qu'un préjudice sérieux soit causé. Il peut également aviser toute personne ou tout organisme susceptible de diminuer ce risque, en ne lui communiquant que les renseignements personnels nécessaires à cette fin sans le consentement de la personne concernée.

Le contenu et les modalités des avis doivent être conformes à la *Loi sur l'accès* et au *Règlement sur les incidents de confidentialité.*

10. ÉVALUATION APPROFONDIE DE LA SITUATION ET PRÉVENTION

Le responsable PRP doit effectuer une évaluation approfondie de l'incident afin d'éviter que de nouveaux incidents de même nature ne se produisent. Cette évaluation approfondie doit être documentée et contenir minimalement les informations prévues à l'annexe 3.

L'évaluation approfondie doit être soumise au comité SI qui doit la réviser et l'approuver avant de la transmettre au pdg, au comité AIPRP et au responsable de la vérification interne.

11. VÉRIFICATION INTERNE

Le responsable de la vérification interne doit évaluer l'efficacité et la performance des mesures mises en place à la suite de chaque incident de confidentialité. Il doit en faire rapport au comité de vérification et des finances.

12. REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

Le responsable PRP doit tenir un registre des incidents de confidentialité conforme au *Règlement sur les incidents de confidentialité.* Il doit transmettre une copie du registre à la Commission si elle le demande.

13. RÔLES ET RESPONSABILITÉS

13.1 Responsable PRP

Le responsable PRP a la responsabilité de :

- effectuer l'évaluation préliminaire;
- convoquer le comité SI;
- effectuer toute déclaration requise par la loi;
- effectuer une évaluation approfondie d'un incident et de proposer des mesures de prévention;
- tenir le registre des incidents de confidentialité;
- assurer la conservation de tout avis, document ou rapport produit en lien avec un incident de confidentialité.

13.2 Comité SI

Le comité SI a la responsabilité de :

- évaluer le risque qu'un préjudice soit causé à une personne;
- déterminer les mesures à prendre et en assurer la mise en œuvre;

- réviser et approuver l'évaluation approfondie et les mesures de prévention;

- se réunir aussi souvent que requis par un incident et documenter ses travaux.

13.3 Direction de la vérification interne

Le responsable de la vérification interne doit évaluer l'efficacité et la performance des mesures mises en place à la suite d'un incident de confidentialité.

13.4 Unités administratives de BAnQ

Les unités administratives de BAnQ impliquées doivent prendre toute mesure urgente requise pour limiter les conséquences d'un incident de confidentialité pour les personnes concernées, notamment la possibilité d'utilisation malveillante de renseignements personnels, l'usurpation ou le vol d'identité. Elles doivent collaborer avec les instances responsables et leur donner accès à tout système informatique, document, dossier, rapport, information ou base de données concernés par un incident de confidentialité.

14. RESPONSABLE DE LA DIRECTIVE

Le secrétaire général et directeur des affaires juridiques est responsable de l'application de la présente directive.

15. ENTRÉE EN VIGUEUR ET RÉVISION

15.1 Entrée en vigueur

La présente directive entre en vigueur le 26 septembre 2022.

15.2 Révision

La révision et la mise à jour de la présente directive sont effectuées au besoin, au minimum tous les cinq ans.

ANNEXE 1 : ÉVALUATION PRÉLIMINAIRE DE L'INCIDENT DE CONFIDENTIALITÉ

Le présent formulaire doit être rempli et transmis au responsable PRP dès qu'une unité administrative a des motifs de croire que s'est produit un incident de confidentialité.

Direction :	
Gestionnaire responsable :	
Date :	

RENSEIGNEMENTS PERSONNELS EN CAUSE	
Description des renseignements personnels touchés (degré de sensibilité, nombre de fichiers ou de données, etc.)	
Support (papier, électronique, etc.)	
PERSONNES CONCERNÉES	
Personnes affectées directement et leur nombre (usagers, employés, etc.)	
Tierces personnes pouvant être concernées (contractants, partenaires, etc.)	
DESCRIPTION DE L'INCIDENT	
Contexte des événements (date, heure, lieu, etc.)	
Circonstances entourant la perte (cause, personnes susceptibles d'être impliquées dans l'incident, etc.)	
MESURES	
Mesures de sécurité physiques et informatiques en place lors de l'incident	
Mesures prises pour limiter les conséquences pour les personnes concernées	

ANNEXE 2 : ÉVALUATION DU RISQUE ET MESURES À PRENDRE

Le comité SI doit procéder à une évaluation du risque et déterminer si des mesures doivent être prises.

ÉVALUATION DU RISQUE
Quelle est la sensibilité des RP? Considérez la nature et la quantité des RP en cause, la possibilité de les combiner avec d'autres renseignements, les personnes concernées, etc.
Cliquez ici pour entrer du texte.
Est-ce que les RP étaient chiffrés ou cryptés? Précisez le type de chiffrement en inscrivant, le cas échéant, la méthode, la norme ou le standard retenu. Précisez les mesures prises pour préserver la confidentialité de la clef de chiffrement et éviter le déchiffrement des données.
Cliquez ici pour entrer du texte.
Est-ce que les RP pourraient être exploités par des personnes malveillantes et quel est le type de préjudice pouvant être causé aux personnes concernées par l'incident? Précisez les types d'utilisation malveillante possibles des RP et les répercussions ou conséquences négatives qui pourraient en résulter. Par exemple : dommage économique ou social (vol et usurpation d'identité ou fraude, perte liée aux affaires, perte d'occasions d'emploi), répercussions sur la santé physique ou psychologique (stress), dommages moraux (atteinte à la réputation, humiliation, diffamation, discrimination).
Cliquez ici pour entrer du texte.
Quel est le niveau de préjudice que pourraient subir les personnes concernées? Précisez : faible, moyen ou élevé en indiquant les faits qui vous amènent à établir ce niveau de préjudice.
Cliquez ici pour entrer du texte.
Est-ce que la situation a un caractère réversible? Par exemple, est-il possible de récupérer les renseignements personnels?
Cliquez ici pour entrer du texte.
Est-ce que des mesures de protection des RP et de sécurité prises immédiatement après la découverte de l'incident ont permis de réduire les risques de préjudices aux personnes concernées et d'atténuer les éventuels effets négatifs de cet incident?
Cliquez ici pour entrer du texte.
Quel est le délai écoulé entre la découverte de l'incident et les mesures prises?
Cliquez ici pour entrer du texte.
MESURES À PRENDRE
Est-ce que d'autres mesures doivent être prises pour réduire les effets de l'incident sur les personnes concernées et les préjudices potentiels pour celles-ci ainsi que pour éviter que ce type d'incident se reproduise? Déterminez les priorités et les mesures à prendre à partir des résultats de l'évaluation des risques.
Cliquez ici pour entrer du texte.

ANNEXE 3 : ÉVALUATION APPROFONDIE DE L'INCIDENT DE CONFIDENTIALITÉ ET PRÉVENTION

Dans son évaluation approfondie de l'incident de confidentialité, le responsable PRP doit minimalement :

- approfondir l'analyse des circonstances de la perte ou du vol des renseignements personnels et effectuer une description chronologique des événements et des mesures prises face à cet incident, incluant les dates et les intervenants concernés;

- répertorier et examiner les normes, politiques ou directives internes en vigueur au moment de l'incident, autant sur le plan de la sécurité informatique, lorsque l'information est en cause, que de la protection des renseignements personnels en général;

- vérifier si ces normes, politiques ou directives internes ont été suivies par les personnes impliquées – déterminer 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 de sécurité et adapter les processus pour éviter qu'un tel incident ne survienne à nouveau;

- évaluer la nécessité d'élaborer une politique en matière de traitement d'une perte ou d'un vol de renseignements personnels au sein de l'organisme ou de l'entreprise;

- formuler des recommandations relatives aux solutions à moyen et long termes et aux stratégies de prévention;

- s'assurer de la réelle nécessité, pour l'organisme ou l'entreprise, de la collecte des renseignements personnels concernés;

- prévoir le suivi devant être accordé.