Approuvée par le conseil d'administration le 27 mars 2023 (RÉS. CA2223A041)

PROCÉDURE RELATIVE À LA GESTION DES INCIDENTS DE CONFIDENTIALITÉ

PRÉAMBULE

Le Conseil des arts et des lettres du Québec recueille et détient des renseignements personnels dans l'exercice de ses attributions et de la mise en œuvre de ses programmes. Il doit prendre les mesures nécessaires pour assurer la protection des renseignements personnels tout au long de leur cycle de vie, soit lors de leur collecte, leur utilisation, leur communication, leur conservation et leur destruction.

La présente procédure détermine un cadre de gestion des incidents de confidentialité au Conseil des arts et des lettres du Québec (Conseil) conforme aux nouvelles obligations en matière de protection des renseignements personnels entrées 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

Les mots et expressions utilisés dans la Procédure ont le sens suivant, sauf stipulation contraire et sauf interprétation contraire imposée par le contexte :

« CAI » : Commission d'accès à l'information du Québec;

« Comité AIPRP » comité sur l'accès à l'information et sur la protection des enseignements personnels mis en place par le Conseil;

« Comité de crise » comité dont la composition et le mandat sont prévus dans le *Cadre de gestion de la sécurité de l'information* et au *Registre d'autorité de la sécurité de l'information* du Conseil

« 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;

Quelques exemples :

- Une ou un membre du personnel 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'infiltre dans un système;
- Une ou un membre du personnel utilise les coordonnées d'une ou d'un usager pour des fins personnelles;
- Un fichier contenant des renseignements personnels concernant une ou un membre du personnel est déposé par erreur dans un répertoire accessible à tout le personnel.
- Une communication de renseignement personnel est effectuée par erreur à la mauvaise personne;

« Personnel » désigne une ou un membre du personnel syndiqué ou non syndiqué du Conseil, qu'elle ou il travaille à temps plein ou à temps partiel, qu'elle ou il soit à l'essai, stagiaire ou contractuel.

« **Procédure** » désigne la présente Procédure relative à la gestion des incidents de confidentialité du Conseil, adoptée par XXXXXXX en vertu de la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (LQ 2021, c 25).

« Renseignement personnel » : tout renseignement qui concerne une personne physique et permet de l'identifier. Le nom d'une personne physique est un renseignement personnel seulement lorsqu'il est mentionné avec un autre renseignement personnel la concernant ou lorsque sa seule mention révélerait un renseignement personnel concernant cette personne;

Quelques exemples de renseignement personnel :

- Le nom d'une personne et sa date de naissance;
- Le nom d'une personne et son numéro de téléphone personnel ou son adresse de domicile;
- Le nom d'une personne et sa demande de bourse au Conseil ou son rapport d'utilisation de bourse;
- Le nom d'une personne et des renseignements de nature financière (carte de crédit, numéro de compte bancaire etc.);

« Responsable de la protection des renseignements personnels » : désigne une ou un membre du personnel nommé à ce titre par la présidence-direction générale conformément à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*;

2. OBJECTIFS

La présente Procédure précise les démarches à effectuer lorsque le Conseil a des motifs raisonnables de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'il détient ou si un tel incident est avéré, et ce, conformément à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1).

La Procédure 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 Procédure s'applique à tous les membres du personnel du Conseil et aux tiers auxquels le Conseil communique des renseignements personnels notamment les membres du conseil d'administration, les membres des comités et jurys, les fournisseurs ou les partenaires du Conseil, incluant les sous-traitants.

4. CADRE RÉGLEMENTAIRE

Le cadre réglementaire de la présente Procédure est notamment composé des lois et règlements suivants :

- 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** »);

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

- le *Règlement sur les incidents de confidentialité.*

5. SIGNALEMENT D'UN INCIDENT DE CONFIDENTIALITÉ

Un signalement doit être fait lorsqu'un motif raisonnable de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel détenu par le Conseil est constaté. Pour ce faire, ce signalement doit être effectué sans délai à la personne Responsable de la protection des renseignements personnels à l'adresse courriel suivante : secretaireduconseil@calq.gouv.qc.ca

La personne signalant l'incident doit indiquer les informations nécessaires pour permettre une analyse adéquate de l'incident en remplissant le formulaire prévu à l'Annexe I.

La ou le responsable de la protection des renseignements personnels effectue une évaluation préliminaire de la situation. Elle ou il peut communiquer avec la personne signalant l'incident afin d'obtenir des informations supplémentaires.

Si elle ou il détermine que la situation correspond à un incident de confidentialité, elle ou il transmet son évaluation préliminaire et l'annexe I aux membres du comité AIPRP.

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

En cas d'incident de confidentialité, les directions 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, la ou le responsable de la protection des renseignements personnels doit convoquer sans délai une séance comité AIPRP 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 AIPRP doit se réunir aussi souvent que requis, selon la gravité de l'incident. Il peut convoquer tout membre du personnel qu'il juge utile et doit documenter ses travaux, notamment en remplissant l'Annexe II.

8. PLAN EN CAS DE CRISE

Si l'incident s'apparente à une crise, la ou le responsable de la protection des renseignements personnels doit communiquer avec la présidence-direction générale afin que celle-ci demande l'intervention du comité de crise qui prendra le relais pour la gestion de l'incident conformément à son mandat.

9. DÉCLARATION DE L'INCIDENT

La ou le responsable de la protection des renseignements personnels doit, avec diligence, aviser la CAI et les personnes concernées par les renseignements personnels si l'incident présente un risque qu'un préjudice sérieux soit causé. Elle ou 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

La ou le responsable de la protection des renseignements personnels 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 III.

L'évaluation approfondie doit être présentée au comité AIPRP et à la présidence-direction générale.

11. VÉRIFICATION INTERNE

La présidence-direction générale est responsable d'évaluer l'efficacité et la performance des mesures mises en place à la suite de chaque incident de confidentialité.

12. REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

La ou le responsable de la protection des renseignements personnels doit tenir un registre des incidents de confidentialité conforme au *Règlement sur les incidents de confidentialité.* Elle ou il doit transmettre une copie du registre à la CAI lorsque celle-ci le demande.

13. RÔLES ET RESPONSABILITÉS

Responsable de la protection des renseignements personnels

La ou le responsable de la protection des renseignements personnels a la responsabilité de :

- effectuer l'évaluation préliminaire;
- demander la convocation du comité AIPRP;
- effectuer toute déclaration requise par la loi;
- effectuer une évaluation approfondie d'un incident et 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.

Comité AIPRP

Le comité AIPRP 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.

Présidence-direction générale

La présidence-direction générale est responsable d'évaluer l'efficacité et la performance des mesures mises en place à la suite d'un incident de confidentialité.

Directions du Conseil

Les directions du Conseil 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

La ou le secrétaire général est responsable de l'application de la présente directive.

15. ENTRÉE EN VIGUEUR ET RÉVISION

La présente directive entre en vigueur dès son adoption par le conseil d'administration . La révision et la mise à jour de la présente directive sont effectuées au besoin, au minimum tous les cinq ans.

ANNEXE I

SIGNALEMENT DE L'INCIDENT DE CONFIDENTIALITÉ ET ÉVALUATION PRÉLIMINAIRE

Le présent formulaire doit être rempli et transmis par courriel au responsable de la protection des renseignements personnels du Conseil (secretaireduconseil@calq.gouv.qc.ca) dès qu'une personne a des motifs de croire qu'un incident de confidentialité s'est produit.

Nom :	
Date :	

RENSEIGNEMENTS PERSONNELS EN CAUSE	
Description des renseignements personnels touchés (degré de sensibilité, nombre de fichier ou de données, etc.)	
Support (papier, électronique, etc.)	
PERSONNES CONCERNÉES	
Personnes affectées directement et leur nombre (usagers, membres du personnel, etc.)	
Tierces personnes pouvant être concernées (contractants, partenaires, etc.)	
DESCRIPTION DE L'INCIDENT	
Contexte des événements (date, heure, lieu, etc.)	
Circonstances entourant la perte ou divulgation (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 II

ÉVALUATION DU RISQUE ET MESURES À PRENDRE

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

ÉVALUATION DU RISQUE
Quelle est la sensibilité des renseignements personnels en cause? Considérer la nature et la quantité des renseignements personnels en cause, la possibilité de les combiner avec d'autres renseignements, les personnes concernées, etc.
Est-ce que les renseignements personnels étaient chiffrés ou cryptés? Préciser 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.
Est-ce que les renseignements personnels pourraient être exploités par des personnes malveillantes et quel est le type de préjudice pouvant être causé aux personnes concernées par l'incident? Préciser les types d'utilisation malveillante possibles des renseignements personnels et les répercussions ou conséquences négatives qui pourraient en résulter (ex. : dommage économique ou social - vol et usurpation d'identité ou fraude, perte liée aux affaires, répercussions sur la santé physique ou psychologique (stress), dommages moraux (atteinte à la réputation, humiliation, diffamation, discrimination).
Quel est le niveau de préjudice que pourraient subir les personnes concernées? Préciser : faible, moyen ou élevé en indiquant les faits qui amènent à établir ce niveau de préjudice.
Est-ce que la situation a un caractère réversible? Par exemple, est-il possible de récupérer les renseignements personnels?
Est-ce que des mesures de protection des renseignements personnels 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?
Quel est le délai écoulé entre la découverte de l'incident et les mesures prises?
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?

Déterminer les priorités et les mesures à prendre à partir des résultats de l'évaluation des risques.

ANNEXE III

ÉVALUATION APPROFONDIE DE L'INCIDENT DE CONFIDENTIALITÉ ET PRÉVENTION

Dans son évaluation approfondie de l'incident de confidentialité, la ou le responsable de la protection des renseignent personnels 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.