PROTECTEUR DU CITOYEN	*Procédure*	**Classification**	**10 pages**
		Émission 2023-01-24	**Dernière révision** 2024-11
			Prochaine révision 2029-11

TITRE : PROCÉDURE SUR LA DÉCLARATION ET LE TRAITEMENT D'UN INCIDENT DE CONFIDENTIALITÉ

RESPONSABLE DE L'APPLICATION	DIRECTION DES AFFAIRES JURIDIQUES ET INSTITUTIONNELLES
DOCUMENTS LIÉS	➢ Politique relative à la sécurité, à la diffusion et à l'accès à l'information ainsi qu'à la protection des renseignements personnels. ➢ Formulaire - Déclaration et traitement d'un incident de confidentialité

OBJECTIF

La procédure décrit les démarches à réaliser pour déclarer et traiter tout incident de confidentialité de façon à éviter ou limiter les préjudices que les citoyens et citoyennes, les membres du personnel ou les instances concernées pourraient subir dans le cadre d'une communication inappropriée de ces données ou renseignements.

CHAMP D'APPLICATION

Cette procédure s'adresse à tous les membres du personnel ainsi qu'aux mandataires de l'institution. Elle vise tout incident relatif à la sécurité de l'information susceptible d'occasionner l'accès à des renseignements personnels ou à des données sensibles ou confidentielles.

CADRE JURIDIQUE

Le Protecteur du citoyen est tenu de prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits, et ce, en vertu 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 concernant le cadre juridique des technologies de l'information* (RLRQ, c. C-1.1) et la *Loi sur les archives* (RLRQ, c. A-21.1).

DÉFINITIONS

Incident de confidentialité portant atteinte à la protection des renseignements personnels : Il s'agit d'un ou de plusieurs événements susceptibles de compromettre la confidentialité des renseignements personnels. Les atteintes à la protection des renseignements personnels peuvent être délibérées ou fortuites. Constituent notamment des incidents :

- L'accès non autorisé à un renseignement personnel
- L'utilisation d'un renseignement personnel à une autre fin que celle prévue lors de la collecte
- La communication non autorisée par la loi
- Le vol, la perte ou la transmission d'un renseignement personnel au mauvais destinataire
- L'organisation est victime d'une cyberattaque (hameçonnage, rançongiciel, etc.)

MODALITÉS D'APPLICATION

Déclaration d'un incident de confidentialité[1]

Lorsque le Protecteur du citoyen a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'il détient, il doit prendre des mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se reproduisent. Les paragraphes suivants décrivent les actions à entreprendre :

1. **Détection** :

   Les membres du personnel ou un mandataire doivent être attentifs aux événements qui constituent des incidents de confidentialité.

2. **Signalement** :

   Lorsqu'un membre du personnel ou un mandataire du Protecteur du citoyen constate un incident, il avise sans délai son gestionnaire.

   Le gestionnaire en informe immédiatement la personne responsable de la protection des renseignements personnels et la personne responsable de la sécurité de l'information.

3. **Confinement**

   Le ou la gestionnaire s'assure que des mesures immédiates sont prises pour contenir l'incident, si nécessaire, par exemple verrouiller la porte, fermer l'ordinateur. Il s'assure également de récupérer les documents auprès des personnes qui les détiennent sans droit et qu'elles n'en ont pas conservés de copie.

[1] Voir annexe 2 pour un tableau récapitulatif

4. **Gestion de l'incident**

   Dès qu'elle est informée d'un incident de confidentialité, la personne responsable de la protection des renseignements personnels et, le cas échéant, la personne responsable de la sécurité de l'information évaluent sommairement la situation (l'annexe 1 présente les éléments à considérer) incluant :

   - L'évaluation du degré de gravité et d'incidence de l'événement;
   - L'évaluation des préjudices pour les personnes concernées;
   - Décision relative à l'information des personnes concernées;
   - Détermination des actions à poser pour gérer l'événement en matière de sécurité, d'informatique, de communication et de PRP.

5. **Convocation du comité de gestion de crise**

   En cas d'incident dont le degré de gravité et d'impact sont majeurs, la personne responsable de la protection des renseignements personnels, de concert avec la personne responsable de la sécurité de l'information, en informe les autorités du Protecteur du citoyen et celles-ci convoquent le comité de gestion de crise en vue de déterminer les actions stratégiques à poser.

   Le Comité de gestion de crise est formé des personnes suivantes :

   - Protecteur ou protectrice du citoyen;
   - Vice-protecteurs ou vice-protectrices;
   - Responsable de la protection des renseignements personnels;
   - Responsable de la sécurité de l'information;
   - Gestionnaire concerné(e);
   - Représentant ou représentante des ressources humaines (volet sécurité physique);
   - Représentant ou représentante des communications;
   - Avocats ou avocates;
   - Répondant ou répondante en matière d'éthique.

6. **Incident présentant un risque qu'un préjudice sérieux soit causé**

   Le comité de gestion de crise élabore un plan de gestion de l'incident en prenant en compte les éléments présentés à l'annexe 1, notamment en matière de sécurité physique, d'informatique, de communication et de protection des renseignements personnels.

   La personne responsable de la protection des renseignements personnels avise la Commission d'accès à l'information en produisant une déclaration d'incident.

   La personne concernée par l'incident doit également être avisée, sauf si cela était susceptible d'entraver une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois.

   Toute personne ou tout organisme susceptible de diminuer ce risque peuvent être avisés, en ne lui communiquant que les renseignements personnels nécessaires à cette fin sans le consentement de la personne concernée.

   Dans ce dernier cas, la personne responsable de la protection des renseignements personnels doit enregistrer la communication au registre approprié.

7. **Bilan de l'incident**

   Avec l'aide de la personne responsable de la protection des renseignements personnels, la personne employée ou la personne mandatée remplit avec diligence la section A du Formulaire – Déclaration et traitement d'un incident de confidentialité.

   La personne responsable de la protection des renseignements personnels évalue ensuite l'efficacité des mesures prises et les moyens mis en place ou proposés afin de prévenir la répétition d'événements similaires en complétant la section B du Formulaire – Déclaration et traitement d'un incident de confidentialité.

8. **Mesures correctives et préventives**

   La personne responsable de la protection des renseignements personnels s'assure de la mise en place des mesures correctives et préventives.

9. **Registre des incidents de confidentialité et des incidents relatifs à la sécurité de l'information.**

   Tous les incidents de confidentialité et les incidents relatifs à la sécurité de l'information sont consignés dans un même registre qui est administré par la personne responsable de la protection des renseignements personnels.

RÔLES ET RESPONSABILITÉS

CAIPRP

- Identifie et tient à jour la liste des membres du comité de gestion de crise.
- Veille à la sensibilisation et à la formation des membres du comité de gestion de crise.

ENTRÉE EN VIGUEUR

Cette politique entre en vigueur le 7 novembre 2024 et doit être révisée tous les 5 ans.

Annexe 1 — Critères d'évaluation

1. Degré de gravité et d'incidence de l'événement (faible, moyen, élevé, critique)

a. À l'égard des personnes concernées

- Peut mettre en péril la sécurité physique de la personne
- Vol d'identité possible
- Sensibilité des renseignements personnels
- Nombre de personnes concernées (important, limité, faible)
- Identification des personnes concernées (connues ou non)
- Renseignements personnels récupérés ou détruits
- Cause de l'incident (vol intentionnel, faute grave ou erreur sans mauvaise foi)
- Risque d'utilisation malveillante
- Perte financière
- Préjudice physique (harcèlement)
- Dommages moraux (atteinte à la réputation, humiliation, diffamation, discrimination)
- Inquiétude, stress

b. À l'égard de l'organisme

- Arrêt d'un ou de plusieurs services critiques pour des clients ou des partenaires
- Violation d'obligations légales ou contractuelles
- Poursuites judiciaires
- Ralentissement des services aux clients ou arrêt d'un service non critique
- Personnes concernées, identifiables ou non
- Renseignements personnels récupérés ou détruits
- Perte financière
- Perte de productivité pour les employés
- Plaintes et recours possibles
- Dommage à la réputation et perte de confiance à l'égard de l'organisme

2. Préjudices prévisibles pour les personnes concernées

- Vol d'identité (susceptible de se produire lorsque la perte concerne le NAS, le numéro de permis de conduire, le numéro de carte de crédit ou bien un ensemble de renseignements révélateurs de l'identité ou d'une situation telle qu'une absence)
- Préjudice physique (risque de menace, harcèlement)
- Dommages moraux (souffrance, humiliation, atteinte à la réputation)
- Répercussions sur la santé psychologique (stress, perte de renseignements de santé, mesures disciplinaires)
- Dommages économiques (perte d'activités commerciales ou de possibilités d'emploi)

- Non-respect de normes professionnelles (pour les membres des ordres professionnels)
- Perte de confiance envers l'organisme (réticence des personnes dans les relations avec l'organisme, client(e)s ou employé(e)s)
- Degré de sensibilité des renseignements personnels perdus
- Cause de l'incident (acte malicieux et vol ou erreur de bonne foi)
- Risque que les renseignements soient utilisés à mauvais escient
- Identification possible ou non des personnes concernées
- Risque de causer davantage de préjudices à la personne (âge, santé mentale ou physique, etc.) s'il y a une notification

3. Éléments du contenu de la notification aux personnes concernées, le cas échéant

- Date de l'événement
- Description de l'événement
- Description des renseignements concernés
- Mesures prises jusqu'à maintenant pour limiter l'atteinte
- Mesures qui seront prises pour éviter la récidive
- Mesures que les personnes peuvent prendre pour éviter les préjudices
- Services offerts par l'organisme pour répondre aux questions et soutenir les personnes concernées, incluant les coordonnées d'une personne-ressource au sein de l'organisme

Annexe 2 — Étapes de gestion d'un incident de confidentialité

Étapes de gestion d'un incident	Actions à prendre	Responsabilités
Signalement	Le responsable de la sécurité de l'information et la responsable de l'accès à l'information et de la protection des renseignements personnels sont informés.	Gestionnaire
Évaluation sommaire et confinement	Information à recueillir auprès du gestionnaire : - Que s'est-il passé ? Quand et comment l'incident est-il survenu ? - L'incident implique-t-il des renseignements personnels ? Quelle est la nature des renseignements personnels visés par l'incident ? Sont-ils des renseignements sensibles ? - Y a-t-il des mesures immédiates à prendre pour réduire l'impact de l'incident et les atteintes à la protection des renseignements personnels ? - Quelle est l'ampleur de l'incident : nombre de dossiers, de documents concernés, de personnes concernées ? Quels sont les risques pour la personne concernée ? - Quelles sont les mesures de sécurité en place ?	RPRP[2] et RSI[3]
Gestion de l'incident dont le degré de gravité et d'impact sont majeurs	Si l'évaluation sommaire conclut qu'il s'agit d'un incident dont le degré de gravité et d'impacts sont majeurs, le comité de crise est convoqué (selon la liste prédéterminée).	RPRP et RSI
	Le comité de crise élabore un plan de gestion de l'incident en tenant compte des éléments suivants :	
	En matière de sécurité physique : - Prévoir des mesures de conservation des preuves, s'il y a lieu - Évaluer la possibilité d'ajouter des dispositifs de sécurité	La personne représentant la DRHA, la personne représentant le service informatique et RSI

[2] Responsable de l'accès à l'information et de la protection des renseignements personnels
[3] Responsable de la sécurité de l'information

	En matière d'informatique : - Vérifier la cause de l'incident, s'il y a lieu - En cas de vol d'ordinateurs ou portables (vérifier les accès, révoquer les accès, détruire à distance le contenu des appareils, identifier les mesures de sécurité présentes sur les appareils)	La personne représentant le service informatique et RSI
	En matière de communication : - Établir un plan de communication - Déterminer l'information à communiquer au membre du personnel - Déterminer le moment et l'information à révéler aux personnes concernées ainsi que le moyen pour le faire - Déterminer les mesures de soutien à fournir aux personnes concernées (ex. CAI, site de GRC, agences de crédit, numéro de téléphone de soutien) - Déterminer si les médias devraient être informés et à quel moment - Déterminer les autorités externes à prévenir et par qui (autorités gouvernementales, autres M/O, fournisseurs externes, agences de crédit, ordre professionnel)	La personne représentant la DECC, RPRP, gestionnaire, RSI, DAJ
	En matière de protection des renseignements personnels : - Obtenir la liste détaillée des renseignements personnels perdus ou volés - Vérifier la possibilité de récupérer les renseignements personnels auprès de ceux qui les détiennent et de s'assurer qu'ils n'en ont pas conservé de copie - Identifier les préjudices que pourraient subir les personnes concernées (dommage économique ou social, usurpation d'identité, perte d'occasion d'emploi, répercussions sur la santé physique ou psychologique) - Identifier les préjudices pour le Protecteur du citoyen - Établir le degré de gravité et d'incidence de l'événement en fonction de la sensibilité des renseignements personnels en cause, du risque d'utilisation malveillante, du contexte et de l'ampleur de l'incident, de la possibilité de plaintes et de recours	RPRP, RSI,
Bilan de la gestion de l'incident	- À l'égard de chaque étape du processus de gestion de l'incident ainsi qu'à l'égard des actions prévues au plan de gestion, poser un diagnostic sur la qualité de la gestion de l'incident (les mesures étaient-elles adéquates ?) et, au besoin, déterminer des mesures correctives visant l'amélioration de cette gestion	RPRP et RSI

	- Faire les suivis des actions retenues au plan de gestion - Remplir la déclaration de l'incident auprès de la Commission d'accès à l'information, s'il y a lieu - Inscrire l'incident au registre des incidents	
Prévention	- En fonction du bilan, déterminer les mesures de précaution ou de prévention à prendre : o à court terme (sur le plan physique, administratif ou informatique) o à long terme (directive sur la gestion d'un incident, directive sur l'utilisation du matériel informatique, directive sur les mesures de sécurité, audit périodique sur la conformité, formation et sensibilisation)	RPRP