KIRKLAND

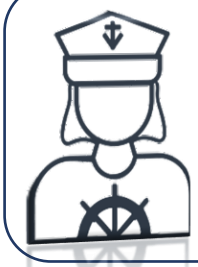
PLAN DE RÉPONSE
INCIDENTS DE CONFIDENTIALITÉ

L'objectif de ce plan de réponse est de présenter les mesures et les étapes effectuées par la Ville de Kirkland (la « Ville ») lors d'un incident de confidentialité[1] impliquant des renseignements personnels[2] et ce, conformément à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.

Rôles et responsabilités

En cas d'incident de confidentialité impliquant des renseignements personnels, la Ville doit intervenir afin de diminuer le risque de préjudice, éviter de nouveaux incidents et tenir un registre de ces incidents.

En cas d'incident de confidentialité, le Comité sur l'Accès intervient afin d'évaluer la situation, enquêter sur celle-ci, évaluer le risque de préjudice, minimiser celui-ci rapidement, effectuer le suivi des mesures de protection afin d'éviter un nouvel incident et remplir le registre. Les rôles et responsabilités des principaux acteurs dans le cadre d'une réponse aux incidents sont présentés ci-dessous.



RPRP (Responsable de la protection des renseignements personnels)

Le RPRP est le greffier(ère) et directeur(trice) des affaires juridiques de la Ville. Lors d'un incident de confidentialité, le RPRP coordonne la mise en place du plan de réponse avec le Comité sur l'Accès.

Le RPRP est le point de contact principal des communications relatives à l'incident et s'assure du respect des obligations légales de la Ville à l'égard de l'incident.

Responsable des technologies de l'information

Le responsable IT s'occupe de tous les aspects techniques de l'incident.

Le responsable IT procède à l'enquête et à l'analyse de l'incident, gère les risques techniques qui y sont associés et met en place des mesures de protection et de récupération adéquates.

Recours à des tiers

Le Comité sur l'Accès a recours à des tiers experts qui le conseille et l'accompagne au besoin (experts en IT, consultants en cyber sécurité, conseillers juridiques, etc.).

1 Constitue un incident de confidentialité la consultation, l'utilisation ou la communication non autorisée d'un renseignement personnel, la perte d'un tel renseignement, ainsi que toute atteinte à sa protection.

2 Constitue un renseignement personnel un renseignement qui, pris seul ou combiné à d'autres, permet d'identifier une personne physique.

Démarche à suivre lors d'un incident de confidentialité

SIGNALEMENT

En cas de soupçon ou d'existence d'un incident de confidentialité, aviser immédiatement le DG, le RPRP, le responsable IT et les autres membres du Comité sur l'Accès.

ÉVALUATION DE L'INCIDENT

Évaluer, enquêter et établir les renseignements compromis, les personnes concernées, la cause et la portée de l'incident.

Évaluer le degré de gravité de l'incident.

Diminuer les risques de préjudice.

ÉVALUATION DU RISQUE DE PRÉJUDICE SÉRIEUX ET SIGNALEMENT

Risque de préjudice sérieux?

Aviser

(art. 63.8 LAI)

OBLIGATOIRE

CAI

OBLIGATOIRE

Personnes concernées

EXCEPTION

Si le signalement est susceptible d'entraver une enquête

(art. 63.8, al.3 LAI)

DISCRÉTION

Personne ou organisme susceptible de diminuer le préjudice

OBLIGATOIRE

Le RPRP doit enregistrer la communication de l'information

(art. 63.8, al. 2 LAI)

Facteurs à considérer lors de l'évaluation du préjudice :

- La sensibilité des renseignements
- Les conséquences appréhendées de leur utilisation
- La probabilité qu'ils soient utilisés à des fins préjudiciables

(art. 63.10 LAI)

INSCRIPTION DE L'INCIDENT DE CONFIDENTIALITÉ AU REGISTRE

(art. 63.11 LAI)

MISE EN ŒUVRE DES MESURES CORRECTIVES ET DE RESTAURATION APPROPRIÉES