Ville de Côte Saint-Luc City of

POLITIQUE - INCIDENT DE CONFIDENTIALITÉ

DÉFINITIONS

Renseignement personnel

Dans un document, sont personnels les renseignements qui concernent une personne physique et permettent de l'identifier.

Incident de confidentialité (« Incident »)

Incident touchant les renseignements personnels conservés par la ville. Plus précisément :

- L'accès, consultation, utilisation ou communication non autorisé par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (la « *Loi* ») d'un renseignement personnel;

- La fuite ou perte de renseignements personnels;

- Toute atteinte à la protection de renseignements personnels. Par exemple :

    - Perte de données provoquée par un virus informatique, piratage, une faille informatique ou une erreur humaine;

    - Envoi d'un courriel à la mauvaise personne;

    - Commérages, etc.

    - Désastre de type inondation ou feu etc.;

Menaces principales aux renseignements personnels :

Humaines :
Une intrusion malveillante dans les services de la municipalité, maladresse d'un employé.

Techniques :
Absence de pare-feu efficace.

Physiques :
Absence de mesures pour limiter les accès aux bureaux, aux salles ou serveurs où sont hébergés les renseignements personnels, locaux mal adaptés pour la conservation de documents.

Prévention des incidents de confidentialité

La Commission d'accès à l'information propose 7 étapes à suivre quant aux mesures de sécurité à mettre en place, afin d'optimiser la prévention d'un incident de confidentialité :

1. Connaître et respecter les obligations en matière de protection des renseignements personnels;

2. Procéder à un inventaire des renseignements personnels détenus et évaluer leur sensibilité;

3. Identifier, analyser et évaluer les risques de survenance d'un incident de confidentialité ainsi que ses impacts potentiels sur la vie privée des personnes concernées. Cette analyse devra se faire dans l'ordre suivant :

    1. Identifier les risques
    2. Déterminer les causes potentielles de ces risques
    3. Évaluer les conséquences potentielles qui découleraient de la matérialisation de ces risques.

4. En fonction des renseignements inventoriés, ainsi que des risques identifiés, déterminer les mesures de sécurité appropriées à mettre en place;

5. Déployer ces mesures de sécurité. Celles-ci doivent être rédigées de façon claire et compréhensible et doivent être facilement accessibles aux personnes qui devront les mettre en œuvre, et à ce titre, être diffusées auprès de tous les employés;

6. Mesurer l'efficacité de ces mesures (par exemple en effectuant des tests de vulnérabilité);

7. Suivre l'application de ces mesures et les réviser au besoin.

Que faire en cas d'incident de confidentialité

Rôles et responsabilité des personnes clés :

- **Responsable de la protection des renseignements personnels (RPRP)**
    - Coordonne la mise en place de la procédure d'intervention, en partenariat avec les services juridiques;
    - Est le point de contact principal des communications en lien avec l'incident;
    - S'assure du respect des obligations légales de la ville à l'égard de l'incident.

- **Spécialiste en technologie de l'information**
    - S'occupe de tous les aspects techniques de l'incident;
    - Procède à l'analyse de l'incident, gère les risques qui y sont associés;
    - Met en place des mesures de protection et de récupération adéquate.

- **Services juridiques**
    - Conseille la ville pour lui permettre de remplir ses obligations légales et pour l'accompagner dans la gestion du risque juridique;
    - Doit être consulté à toutes les étapes de la gestion de l'incident pour garantir la préservation du secret professionnel.

Procédure d'intervention suivant un incident de confidentialité : 7 étapes

1. Identification

Tout employé qui découvre ou soupçonne l'existence d'un incident doit en aviser immédiatement le RPRP ou son superviseur immédiat. Si la personne avisée n'est pas le RPRP, elle doit aviser ce dernier dès que possible.

La présence aux réunions devrait être limitée à certaines personnes et la diffusion des procès-verbaux et de tout document ou toute autre communication à l'extérieur des réunions de gestion des incidents.

2. Évaluation initiale de la situation

Pour évaluer un incident, le RPRP doit se poser les questions suivantes :

- Quels renseignements sont compromis?
- Qui sont les personnes concernées?
- Quelle est la cause et la portée de l'incident?
- Quel est le risque de préjudice lié à cet incident?

Suite à l'évaluation, un degré de gravité est attribué à l'incident potentiel. Cette évaluation doit être révisée régulièrement au cours du processus d'intervention. Le tableau de classement des incidents ci-dessous présente divers facteurs devant aider le RPRP à classer un incident. Certains facteurs ne s'appliquent pas nécessairement à tous les incidents (voir tableau p.4).

Si un incident présente des caractéristiques qui correspondent à plusieurs colonnes de gravité, la gravité de l'incident correspond à la gravité la plus élevée. Le classement des incidents est un processus dynamique. La gravité d'un incident peut évoluer au fur et à mesure que l'enquête révèle de nouveaux détails. Le classement des incidents doit être effectué en étroite collaboration avec les services juridiques. Il ne lie aucunement la municipalité et ne constitue aucunement une conclusion ou un aveu de quelque nature.

Facteurs relatifs à l'incident	Degré de gravité de l'incident		
	1er degré	2e degré	3e degré
Effets sur les personnes concernées et les systèmes	Touche peu de personnes ou de systèmes	Effet à l'échelle d'un service	Effet à l'échelle de la municipalité
Effets sur le public	Aucun	Effet potentiel	Effet indéniable
Mesures de remédiation	Solutions disponibles	Faibles mesures de remédiation	Aucune mesure de remédiation
Chiffrement ou anonymisation des renseignements touchés	Algorithme de chiffrement et contrôle par clés robustes	Algorithme et/ou contrôle par clés faibles	Aucun chiffrement, ou chiffrement facilement déchiffrable
Procédure de résolution des problèmes techniques	Disponible et bien définie	Procédure de résolution mal définie, solutions disponibles	Aucune procédure de résolution ni aucune autre solution disponible
Sensibilité des renseignements	Faible	Moyenne	Élevée
Incident devant potentiellement être signalé à la CAI, aux personnes concernées ou une autorité de règlementation ou agence d'application de la *Loi*	Non	Possible	Oui

3. Enquête

Le RPRP, de concert avec les services juridiques, coordonne la collecte et la préservation des éléments de preuve, afin de répondre aux questions « **qui**, **quoi**, **quand**, **où**, **pourquoi** et **comment** » à l'égard de chaque incident. L'objectif est de déterminer la cause fondamentale de l'incident, son étendue et ses effets. La municipalité pourrait devoir procéder à une enquête de cybersécurité et interroger tout employés ayant connaissance de l'incident.

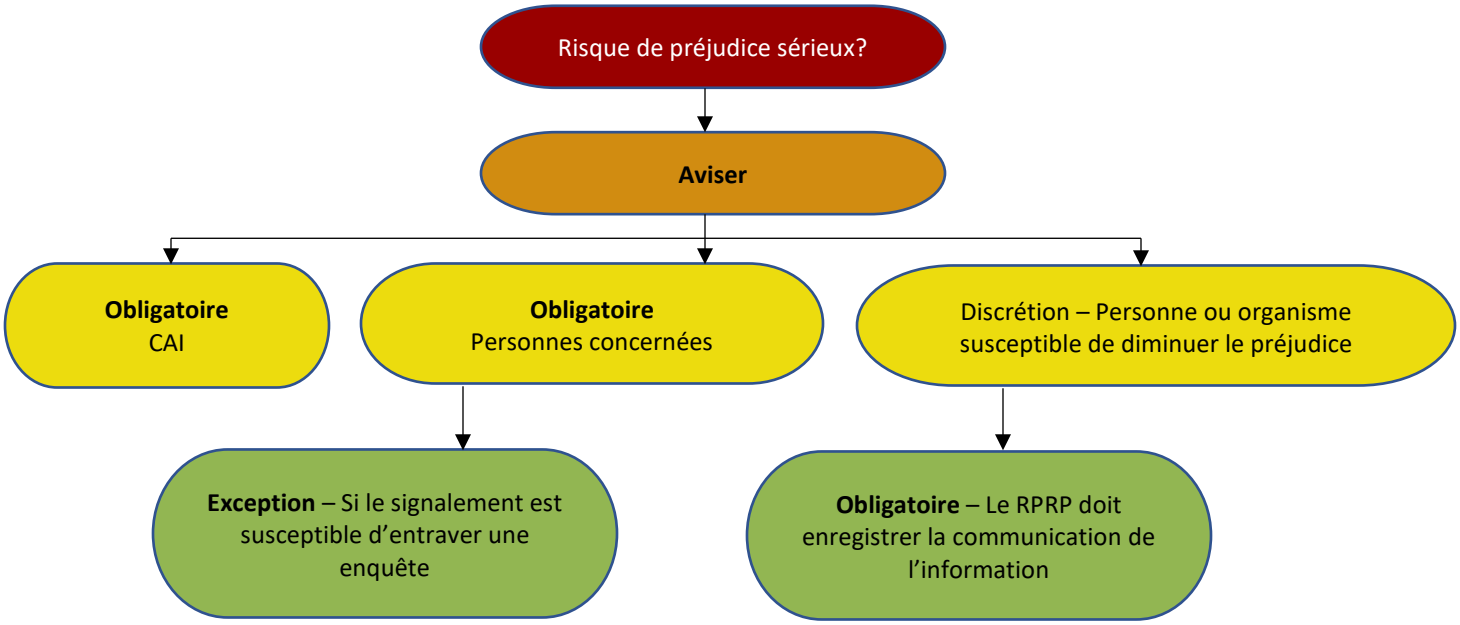
4. Recours à des tiers

Dans certains cas, Le recours à des tiers, comme des consultants en cyber sécurité, peut se montrer nécessaire et approprié. Le RPRP doit tenir compte des exigences de la police d'assurance, car certains assureurs préfèrent faire affaire avec des conseillers qu'ils ont autorisés ou pour lesquels leur approbation est nécessaire.

Le RPRP assure le suivi continu de l'évaluation et de l'enquête initiales afin de déterminer si quelque chose d'autre peut être fait pour mitiger les effets de l'incident et y mettre fin. Les activités doivent être rétablis le plus rapidement

possible, pourvu que cela n'engendre pas d'autres problèmes de sécurité, n'expose pas la ville à un risque d'incidents additionnels ou n'entraine pas la perte ou destruction involontaire d'éléments de preuve.

5. Évaluation du risque de préjudice sérieux et signalement



Afin d'établir si la ville doit aviser la CAI ou les personnes concernées, il faut procéder à l'**évaluation du risque de préjudice**. À cette étape, le RPRP doit être consulté; la ville a des obligations de signalement seulement lorsque l'incident présente un risque de préjudice sérieux pour les personnes concernées.

Dans le cadre de cette évaluation, la ville doit notamment tenir compte des éléments suivants :

- La **sensibilité** des renseignements concernés par l'incident :
  Plus le degré de sensibilité est élevé, plus le risque que le préjudice soit sérieux est important.
- Les **conséquences** appréhendées de leur utilisation :
  Ex : si des renseignements d'identité on été extrait (no d'assurance sociale, nom ou adresse d'une personne), le vol d'identité ou une fraude financière pourraient en résulter.
- La **probabilité** qu'ils soient utilisés à des fins préjudiciables :
  Ex. : les éléments suivants indiquent la probabilité haute ou faible que les renseignements soient utilisés à des fins préjudiciables :

HAUT RISQUE	FAIBLE RISQUE
L'incident de confidentialité résulte d'un acte intentionnel (par opposition à une divulgation accidentelle).	Les renseignements sont entre les mains d'entités restreintes ou connues qui se sont engagées à détruire ou ne pas divulguer les renseignements.
Une entité malveillante ou qui présente un risque pour la réputation de la personne concernée a pris possession des renseignements personnels.	Les renseignements ont été exposés à des personnes ou des entités peu susceptibles de les communiquer de façon préjudiciable (ex. : dans le cadre d'une communication accidentelle à un mauvais destinataire).
Les renseignements ont été communiqués à un nombre important de personnes.	Les renseignements compromis ou inaccessibles ont été récupérés.
Les renseignements n'ont pas pu être récupérés.	Les renseignements sont adéquatement chiffrés, anonymisés ou autrement difficiles d'accès.
Les renseignements sont facilement accessibles (ex. : en l'absence de chiffrement adéquat).	
Un préjudice s'est effectivement matérialisé.	

- La quantité de renseignements impliqués et le nombre de personnes visées.

Si, à la suite de l'évaluation, la municipalité conclut à la présence d'un tel risque, elle devra alors aviser rapidement la CAI et les personnes dont les renseignements personnels sont concernés par l'incident de confidentialité.

Si les personnes concernées doivent être avisées, le RPRP et les services juridiques déterminent également le mode et les détails de l'avis conformément à la *Loi*. Afin de faciliter la mise en œuvre de ces obligations de signalement, vous trouverez des modèles d'avis à la CAI et aux personnes concernées, en annexe 1 et 2 de ce Guide.

D'autres signalements ou communications pourraient être nécessaires ou utiles dans le cadre de la gestion de l'incident, par exemple, à vos partenaires d'affaires et fournisseurs de services, à certaines autorités, comme les services de police et vos assureurs.

Une fois l'enquête terminée, le RPRP fait un rapport sur l'incident aux intervenants concernés, conformément aux lois applicables, et en collaboration avec les services juridiques.

6. Tenue du registre et prévention

Quelle que soit la gravité apparente de l'incident, le RPRP doit documenter l'incident de confidentialité qui vise des renseignements personnels. La ville doit notamment conserver les informations suivantes :

- **Détails de l'incident**, y compris ses causes, ce qui s'est passé et les renseignements personnels affectés : date avérée ou estimée de l'Incident;

description des circonstances de l'Incident; nombre de personnes touchées; nature des renseignements concernés;
- **Effets et conséquences de l'incident**; Incident signalé à la CAI et/ou aux individus (si non, quels éléments permettent de conclure que l'Incident n'a pas occasionné de risque de « préjudice sérieux » au sens de la Loi;
- **Atteinte signalée à toute personne ou tout organisme susceptible de diminuer le risque de préjudice sérieux** (à qui le signalement a été fait, en quoi la personne/organisme sont à même de diminuer le risque, quelle information a été communiquée;
- **Mesures correctives prises**;
- **Justification des décisions prises en réponse à l'incident**, en particulier dans le cas d'un incident qui n'est pas signalé à la CAI ou aux personnes concernées.

Le registre, ainsi que tous les documents en lien avec l'Incident doivent être conservés selon le calendrier de conservation de la ville.

Une fois les mesures prises afin de limiter et atténuer les risques associés à l'incident, la mise en place de mesures de protection à long terme peut être nécessaire. On examine s'il y a lieu de procéder à la vérification des protocoles de sécurité techniques et physiques, selon le cas. Le RPRP révise et actualise les politiques de la ville en tenant compte des leçons tirées de l'enquête sur l'incident.

Également, le personnel reçoit une formation sur les obligations en matière de protection de la vie privée et des renseignements personnels qu'impose la *Loi* à la ville.

7. Récupération

Une fois l'incident circonscrit et éradiqué, la ville doit mettre en œuvre les mesures correctives et de restauration appropriées :

- Réinstallation du système d'exploitation;
- Restauration des systèmes à partir de sauvegardes propres;
- Réorganisation des systèmes;
- Restriction des accès aux dossiers papiers et numériques en fonction des tâches et responsabilités de chaque employé;
- Nettoyage des fichiers si nécessaire;
- Mise à jour des routeurs ou des pares-feux si nécessaire;
- Installation des correctifs de sécurité;
- Suppression des vulnérabilités;
- Reconnexion au réseau;
- Validation des fonctions du système.

Ville de City of
Côte Saint-Luc

POLICY – CONFIDENTIALITY INCIDENT

DEFINITION

Personal Information

In a document, information that relates to a natural person and allows that person to be identified.

Confidentiality Incident (“Incident”)

Incidents involving personal information held by the City. More specifically:

- Access, consultation, use or release of personal information not authorized by the *Act respecting Access to Documents held by public bodies and the Protection of personal information* (the *“Act”*);

- Leakage or loss of personal information;

- Any breach of the protection of personal information. For example:

    - Loss of data caused by a computer virus, hacking, computer security breach or human error;

    - An email directed to the wrong person;

    - Gossips, etc.

    - Disasters such as flood or fire, etc.

Main threats to personal information

Human:
Malicious intrusion in the services of the municipality, employee blunder;

Technical:
No effective firewall;

Physical:
Lack of measures to limit access to offices, rooms or servers where personal information is housed, poorly adapted premises for storing documents.

Confidentiality Incident Prevention

The *Commission d'accès à l'information* proposes 7 steps to take regarding security measures to put in place in order to optimize prevention of confidentiality Incidents:

1. Know and fulfill the obligations regarding the protection of personal information;

2. Prepare an inventory of personal information held and assess their sensitivity;

3. Identify, analyze and assess the risks of a privacy Incident and its potential impact on the privacy of individuals concerned. This analysis should be done in the following order :

    1. Identify the risks
    2. Determine the potential causes of these risks
    3. Assess the potential consequences that would result from the occurrence of these risks.

4. Based on the results of the personal information inventory and the risks identified, determine the appropriate security measures to put in place;

5. Implement these security measures, which must be written in a clear and understandable way and be easily accessible to the people who will have to enforce them, and as such, be distributed to all employees;

6. Assess the effectiveness of these measures (for example by conducting vulnerability tests);

7. Monitor the implementation of these measures and revise them as needed.

What to do in case of a confidentiality Incident

Roles and responsibilities of key personnel:

- **Person in charge of the protection of personal information (PCPPI)**
    - Coordinates the implementation of the Incident response procedure, in conjunction with Legal Services;
    - Is the primary point of contact for communications related to the Incident;
    - Ensures compliance with the City's legal obligations with respect to the Incident.

- **Information technology specialist**
    - Handles all the technical aspects of the Incident;
    - Reviews the Incident and manages the associated risks;
    - Implements adequate protection and recovery measures.

- **Legal Services**
    - Advises the City on how to fulfill its legal obligations and to assist in the management of the legal risk;
    - Must be consulted at all stages of Incident management to ensure that professional secrecy is maintained.

Response procedure following a confidentiality Incident: 7 steps

1. Identification

Any employee who discovers or suspects that an Incident has occurred must immediately notify the PCPPI or his/her immediate supervisor. If the person notified is not the PCPPI, he/she shall notify the PCPPI as soon as possible.

Attendance at meetings should be limited to selected individuals. The same applies to the dissemination of minutes and any documents or other communications outside of Incident management meetings.

2. Initial assessment of the situation

To assess an Incident, the PCPPI must ask the following questions:

- What information is compromised?
- Who are the individuals involved?
- What is the cause and scope of the Incident?
- What is the risk of harm associated with this Incident?

Following the assessment, a severity level is assigned to the potential Incident. This assessment must be reviewed regularly during the response process. The Incident classification chart below outlines various factors that should assist the PCPPI in classifying an Incident. Some factors may not apply to all Incidents (see table on page 4).

If an Incident has characteristics that correspond to more than one severity column, the severity of the Incident corresponds to the highest severity. Incident ranking is a dynamic process. The severity of an Incident may change as the investigation reveals new details. The classification of Incidents should be done in close consultation with Legal Services. It is not binding on the City and does not constitute a conclusion or admission of any kind.

Factors related to the Incident	Severity of the Incident		
	1st level	2nd level	3rd level
Impacts on the individuals involved and the systems	Affects few people or systems	Department-wide impact	Citywide effect
Impacts on the public	None	Potential impact	Undeniable impact
Remediation measures	Solutions available	Poor remediation measures	No remediation measures
Encryption or anonymization of affected information	Strong encryption algorithm and key control	Weak algorithm and/or key control	No encryption, or easily decrypted encryption
Technical problem resolution procedure	Available and well defined	Poorly defined resolution procedure, solutions available	No resolution procedure or other solution available
Sensitivity of the information	Low	Moderate	High
Incident potentially reportable to *CAI*, affected individuals, or a regulatory authority or enforcement agency of the *Act*	No	Possibly	Yes

3. Investigation

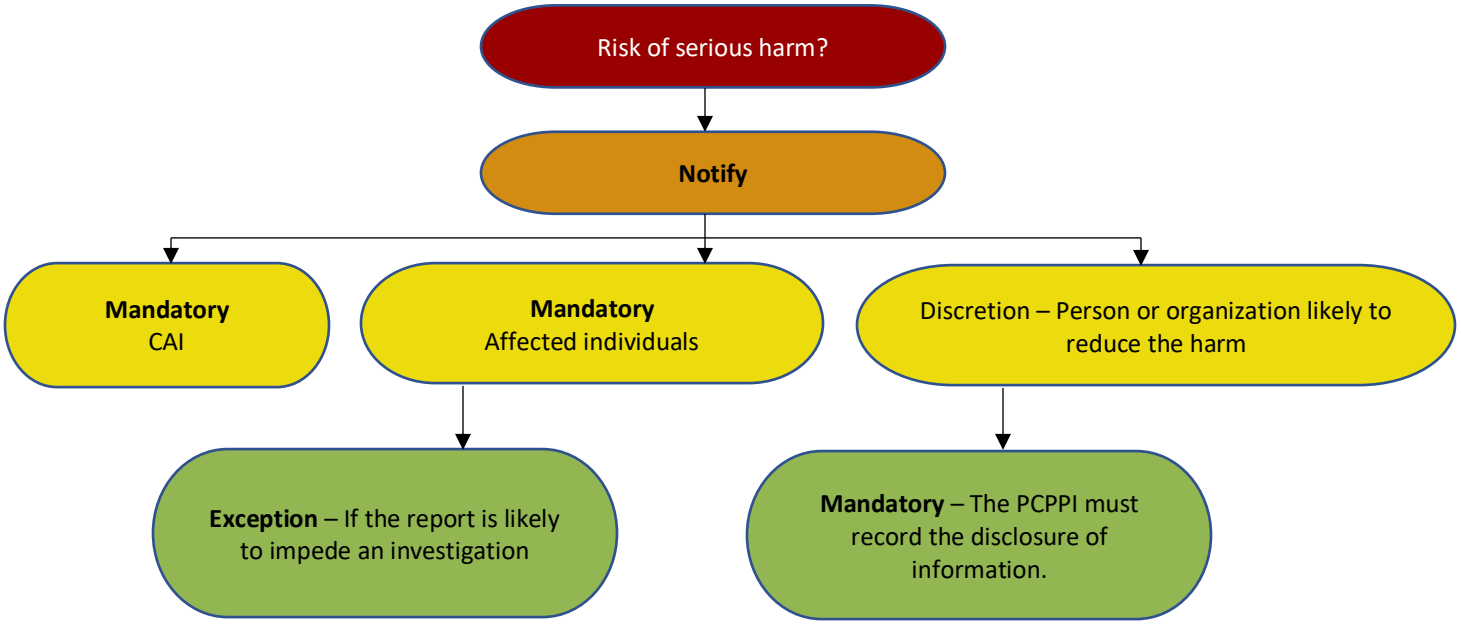
The PCPPI, in conjunction with Legal Services, coordinates the collection and preservation of evidence to answer the "**Who, What, When, Where, Why and How**" questions for each Incident. The goal is to determine the root cause of the Incident, its extent and impacts. The municipality may need to conduct a cybersecurity investigation and question any employees with knowledge of the Incident.

4. Use of Third Parties

In some cases, the use of third parties such as cybersecurity consultants may be necessary and appropriate. The PCPPI has to consider the requirements of the insurance policy, as some insurers prefer to deal with consultants they have authorized or for whom their approval is required.

The PCPPI shall ensure ongoing follow-up to the initial assessment and investigation to determine if anything else can be done to mitigate and stop the effects of the Incident. Operations shall be restored as quickly as possible, provided this does not create additional safety issues, expose the City to the risk of additional Incidents, or result in the inadvertent loss or destruction of evidence.

5. Assessing the risk of serious harm and reporting



In order to determine whether the City must notify the CAI or the individuals involved, an **assessment of the risk of harm** must be conducted. At this stage, the PCPPI should be consulted; the City has reporting obligations only when the Incident poses a serious risk of harm to the individuals concerned.

As part of this assessment, the City should consider the following:

- The **sensitivity** of the information concerned by the Incident:
  The greater the degree of sensitivity, the greater the risk of serious harm.
- The anticipated **consequences** of its use:
  Ex: If identity information has been extracted (social insurance number, name or address of an individual), identity theft or financial fraud could result.
- The **likelihood** that such information will be used for injurious purposes:
  Ex : The following elements indicate the high or low probability that the information will be used for harmful purposes:

HIGH RISK	LOW RISK
The confidentiality Incident results from an intentional act (as opposed to an accidental disclosure).	The information is in the hands of restricted or known entities that have agreed to destroy or not disclose the information.
A malicious entity or one that poses a risk to the individual's reputation has taken possession of the personal information.	The information was exposed to individuals or entities unlikely to disclose it in a harmful manner (e.g., through accidental disclosure to the wrong recipient).
The information was shared with a significant number of individuals.	The compromised or inaccessible information has been recovered.
The information could not be retrieved.	The information is properly encrypted, anonymized or otherwise difficult to access.
The information is easily accessible (ex: in the absence of proper encryption).	
A prejudice has effectively materialized.	

- The amount of information involved and the number of individuals affected.

If, as a result of the assessment, the municipality concludes that such a risk exists, it shall promptly notify the CAI and the individuals whose personal information is affected by the confidentiality Incident.

If the individuals concerned have to be notified, the PCPPI and Legal Services will also determine the mode of notification and the details of the notice in accordance with the *Act*. To assist in the implementation of these reporting obligations, sample notices to the CAI and affected individuals are included in Annex 1 and Annex 2 of this Guide.

Other reports or communications may be necessary or useful in managing the Incident, for example, to your business partners and service providers, to certain authorities, such as police services and your insurers.

Once the investigation is complete, the PCPPI will report the Incident to all stakeholders concerned, in accordance with applicable laws and in collaboration with Legal Services.

6. Maintenance of the register and prevention

Regardless of the apparent severity of the Incident, the PCPPI shall document the privacy Incident involving personal information. In particular, the City shall keep the following data:

- **Details of the Incident**, including what caused it, what happened, and what personal information was affected: the actual or estimated date of the Incident; a description of the circumstances of the Incident; the number of people affected; the nature of the information involved;

- **Effects and consequences of the Incident**; Incident reported to the CAI and/or individuals (if not, what evidence is there to conclude that the Incident did not result in a risk of "serious harm" as defined in the Act);
- **Reported harm to any person or organization that could reduce the risk of serious harm (**to whom the report was made, how the person/organization can reduce the risk, what information was provided);
- **Corrective measures implemented;**
- **Rationale for decisions made in response to the Incident,** particularly in the case of an Incident that is not reported to the CAI or to the individuals involved.

The register, along with all documents related to the Incident, shall be retained in accordance with the City's retention schedule.

Once steps have been taken to limit and mitigate the risks associated with the Incident, long-term safeguards may need to be put in place. Consideration is given to whether technical and physical security protocols should be audited, as appropriate. The PCPPI reviews and updates the City's policies taking into account lessons learned from the Incident investigation.

In addition, staff receives training on the City’s privacy and personal information protection obligations under the *Act*.

7. Recovery

Once the Incident is contained and eradicated, the City must implement appropriate remedial and restoration measures:

- Reinstallation of the operating system;
- Restore systems ffrom clean backups;
- Reorganization of systems;
- Restriction of access to paper and digital files according to the tasks and responsibilities of each employee;
- Cleanup of files if necessary;
- Updating routers or firewalls if necessary;
- Installation of security patches;
- Removal of vulnerabilities;
- Reconnecting to the network;
- Validation of system functions.