RESPONSE PLAN
CONFIDENTIALITY INCIDENT

The objective of this response plan is to present the measures and steps taken by the Town of Kirkland (the “Town”) during a confidentiality incident[1] involving personal information[2], in accordance with the *Act respecting Access to documents held by public bodies and the Protection of personal information*.

Roles and Responsibilities

In the event of a confidentiality incident involving personal information, the Town must intervene to reduce the risk of harm, avoid new incidents and keep a record of these incidents.

In the event of a confidentiality incident, the Access Committee intervenes to evaluate the situation, investigate it, evaluate the risk of harm, minimize it quickly, monitor protective measures to avoid a new incident and complete the registry. The roles and responsibilities of key players in an incident response are presented below.

ORAD (0fficer Responsible for Access to Documents)

The ORAD is the Town Clerk and Director of legal affairs of the Town. During a confidentiality incident, the ORAD coordinates the implementation of the Response Plan with the Access Committee.

The ORAD is the primary point of contact for incident communications and ensures that the Town’s legal obligations with respect to the incident are met.

IT Manager

The IT Manager deals with all technical aspects of the incident.

The IT Manager investigates and analyses the incident, manages the associated technical risks and implements adequate protection and recovery measures.

Third-party assistance

The Access Committee uses third-party experts who advise and support it as needed (IT experts, cybersecurity consultants, legal advisors, etc.).

[1] The unauthorized access, use or disclosure of personal information, the loss of such information or any other breach of the protection of personal information.

[2] Personal information is information which, taken alone or in combination with other information, makes it possible to identify a natural person.

Steps to Complete in a Confidentiality Incident

REPORTING

In the event of suspicion or existence of a confidentiality incident, notify immediatly the DG, the ORAD, the IT manager and the other members of the Access Committee.

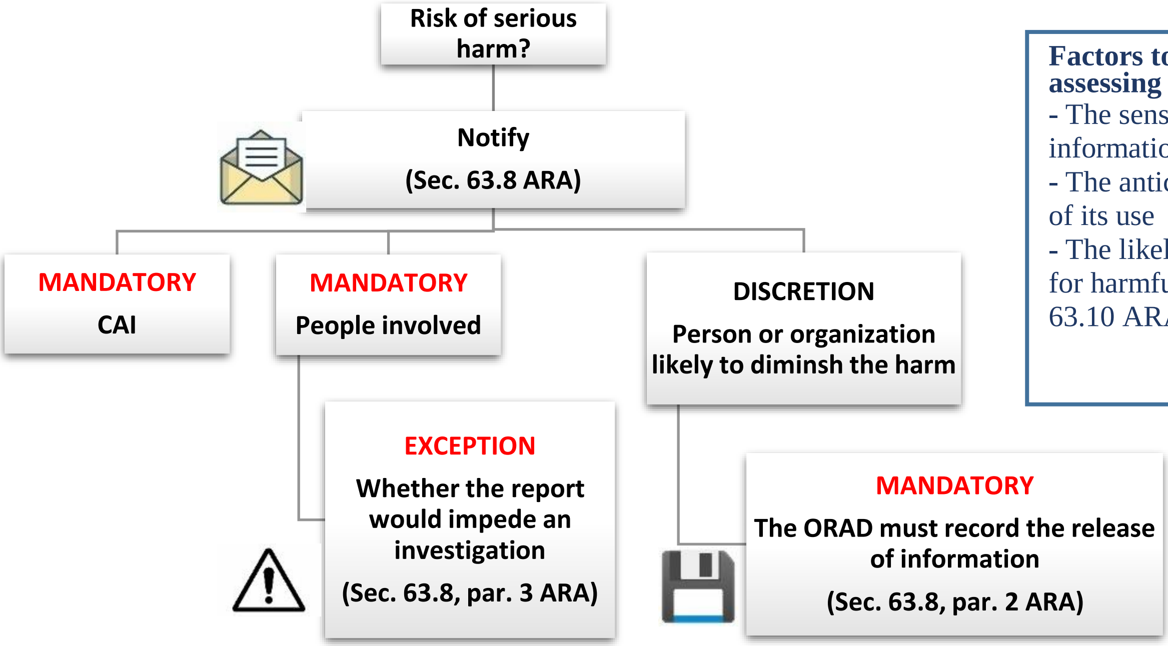
INVESTIGATION OF THE INCIDENT

Establish the compromised information, the people involved, the cause and scope of the incident.

Assess the severity of the incident.

Reduce the risks of harm.

SERIOUS HARM RISK ASSESSMENT AND REPORTING



Risk of serious harm?

Notify

(Sec. 63.8 ARA)

MANDATORY

CAI

MANDATORY

People involved

EXCEPTION

Whether the report would impede an investigation

(Sec. 63.8, par. 3 ARA)

DISCRETION

Person or organization likely to diminsh the harm

MANDATORY

The ORAD must record the release of information

(Sec. 63.8, par. 2 ARA)

Factors to consider when assessing the damage:

- The sensitivity of the information
- The anticipated consequences of its use
- The likelihood that such use is for harmful purposes (Sec. 63.10 ARA)

RECORDING OF THE CONFIDENTIALITY INCIDENT IN THE REGISTRY

(Sec. 63.11 ARA)

IMPLEMENTATION OF APPROPRIATE CORRECTIVE AND RESTORATION MEASURES