Commission
d'accès à l'information
du Québec

CHECKLIST
FOR ORGANIZATIONS AND COMPANIES

WHAT TO DO IN CASE OF LOSS OR THEFT OF PERSONAL INFORMATION

The law respecting access to documents held by public bodies and the protection of personal information and the law on the protection of personal information in the private sector impose obligations on public bodies and private companies concerning the collection, retention, use and communication of personal information.

In general, personal information held by a company or organization is confidential, except as prescribed by law. Organizations and companies are obliged to take security measures to protect personal information.

The Commission d'accès à l'information is convinced that adequate security measures help reduce the risk of the inappropriate use or disclosure of personal information.. However, a loss or theft of personal information may occur and risk the confidentiality of information.

When a loss of personal information occurs, one of the concerns of the Commission d'accès à l'information is to ensure that the company or organization takes the necessary measures to prevent or limit harm done to the individuals concerned with the breach in their personal information and what they may suffer as a result. Promptly informing the individuals concerned is an effective way to limit or even prevent any harm.

It is also essential that adequate security measures are taken to prevent a re-occurrence of such incidents. The Commission d'accès à l'information can accompany you and advise you in your efforts.

This checklist is a tool that the Commission d'accès à l'information provides to organizations and companies to help them assess the situation when there is a loss or theft of personal information. It is a guide and the main steps mentioned are not exhaustive.

Québec (Headquarters)
Bureau 1.10
575, rue Saint-Amable
Québec (Québec) G1R 2G4
Telephone : 418 528-7741
Fax : 418 529-3102

Montréal
Bureau 900
2045, rue Stanley
Montréal (Québec) H3A 2V4
Telephone : 514 873-4196
Fax : 514 844-6170

You can call both offices toll free at : 1 888 528-7741

E-mail:cai.communications@cai.gouv.qc.ca

Website: www.cai.gouv.qc.ca

MAIN STEPS TO FOLLOW WHEN THERE IS A LOSS OR THEFT OF PERSONAL INFORMATION

STEP 1 : PRELIMINARY EVALUATION OF THE SITUATION

1. **Briefly define the context of the loss or theft of personal information :**

    - Identify the personal information affected as well as supporting information;
    - Identify the people, number of people as well as the group of people (customers, employees, etc.) affected;
    - Establish the context of events (date, hour, place, etc.);
    - If possible, identify the circumstances surrounding the loss, (cause, people likely to be involved in the incident, etc.);
    - List the physical and computer security measures in place during the incident.

2. **Inform outside authorities concerned that must be advised immediately of the incident (before risk evaluation) :**

    - Police department (if circumstances suggest the possibility of a crime);
    - Commission d'accès à l'information.

3. **Designate a person or team to be in charge of the situation.**

4. **Inform internal responders concerned :**

    - Organization or company leaders;
    - Person in charge of administrative unit concerned;
    - Person in charge of the protection of personal information;
    - Legal Counsel;
    - Communications management (media management and customer phone calls).

STEP 2 : LIMIT INVASION OF PRIVACY

The organization or company must take immediate and appropriate measures to limit the consequences for the people concerned about the possibility of the malicious use of their personal information, including theft or identity theft :

1. **1. Take immediate measures to limit the consequences of the loss or theft of personal information by ensuring to end the non-compliant practice, if applicable;**
2. **Recover physical or digital files, as the case may require;**
3. **Revoke or modify passwords or computer access codes;**
4. Control weaknesses in computer systems.

STEP 3 : ASSESSING THE RISKS

1. **Complete a preliminary risk assessment by considering the sensitivity of personal information involved, taking into account the nature, the quantity, the possibility of combining it with other information, the people involved, etc.;**

2. **Determine the context of the incident including :**

    - The cause (e.g.: the deliberate or non-deliberate theft of personal information, human error, a computer breach, etc.);
    - The known or probable authors of lost or stolen personal information (e.g. criminal organizations, the general public, etc.);
    - The extent of the situation (number of people affected and sectors affected);
    - The systemic or non-systemic nature of the loss of personal information (especially when the loss is directly generated by human intervention);
    - A probability assessment of the likelihood of a similar event happening again.

3. **Evaluate the possibility that the personal information concerned could be detrimental to the individuals concerned, taking into account, and in particular, the security measures taken to protect them, their access difficulty and intelligibility (password, encryption, etc.);**

4. **Evaluate the reversible or irreversible nature of the situation, including the possibility of retrieving personal information;**

5. **Assess whether the immediate measures taken were adequate to limit harm and complete them, if necessary;**

6. **Determine potential harm, including assessing the potential future use of personal information by malicious individuals, in particular, identity theft;**

7. **Determine priorities and identify actions to take based on assessment results of these risks.**

STEP 4 : NOTIFY THE ORGANIZATIONS AND INDIVIDUALS CONCERNED

1. **Determine who should be made aware of the loss or theft of personal information on the basis of risk assessment:**

    - Police department : in cases where the losses can result in the committing of a crime, the police department must first be notified of the facts surrounding the disappearance, and then all the other subsequent steps. It is important to pay close attention so as not to impede the investigation and to protect evidence that may be relevant;
    - People concerned : if the loss or theft of personal information Presents a risk of harming the individuals concerned, They should be notified immediately. It is not about alarming them, but rather warning them so that they can take appropriate measures to protect their personal information;
    - Commission d'accès à l'information: if the individuals concerned by personal information are from Quebec, the Commission could initiate an inspection or an investigation and play an advisory role in searching for solutions;
    - Other : it may also be necessary to inform other responders such as credit bureaus, authorized agents, co-contractors, government authorities, trade unions, professional associations, etc.

    However, in the dissemination of information regarding the loss of personal information, special attention should be paid not to increase harm that may occur to the individuals concerned (e.g. : minimize the amount of personal information in the advisory).

2. **Designate the people in charge to inform previously identified outside responders as well as the time and the means (letter, e-mail, telephone);**

3. **If applicable, identify and record the reasons behind the decision not to notify the individuals concerned and other responders.**

NOTICE TO INDIVIDUALS AFFECTED BY A LOSS OR THEFT OF THEIR PERSONAL INFORMATION

Depending on circumstances, it may be necessary to notify the victims of the loss or theft of their personal information. This advisory may include some of the following elements:

- The context of the incident and when it occurred, and a description of the nature of the personal information affected, without disclosing specific personal information;
- A brief description of measures taken to minimize or prevent harm, as well as a list of individuals who have been informed of the situation (Police department, (Commission d'accès à l'information, etc.);
- Actions taken by organizations and companies to help people concerned (Assistance and information service, credit alert subscription, etc.);
- Measures that individuals may take to reduce risk of harm or to better protect themselves (refer to document "Identity Theft", available from the Commission d'accès à l'information);
- Other general information documents designed to help people guard against identity theft;
- Contact information of an organization representative who can answer questions and to report to;
- Main measures to be taken to avoid a recurrence of the situation (change in practice or procedures, staff training, policy revision or development, verification, periodic monitoring, etc.).

STEP 5 : IN-DEPTH ASSESSMENT OF THE SITUATION AND PREVENTION

1. **Go further with the analysis of circumstances regarding the loss or theft of personal information and chronologically describe events and actions taken in response to this incident, including dates and responders;**

2. **List and review standards, policies or internal guidelines in place at the time of the incident, both in terms of computer security, when information is involved, as well as general personal information;**

3. **Verify whether these standards, policies or internal guidelines have been followed by the people involved; identify the reasons why they were not followed, where appropriate;**

4. **If it is a procedural error or operational failure, record them in the security file and adapt procedures to avoid such an incident from happening again;**

5. **Assess the need to develop a policy for processing the loss or theft of personal information within an organization or company;**

6. **Formulate recommendations related to medium and long-term solutions and prevention strategies;**

7. **Ensure the real need for the organization or company, to gather personal information;**

8. **Plan monitoring before it is given.**

STEP 6 : MONITORING

It is important to monitor :

- processing procedures that must be applied when there is a loss or theft of personal information and results obtained in order to improve them, if need be;
- security measures required following the incident and their performance;
- communication of relevant information to the Commission d'accès à l'information and police department involved, where appropriate.

April 2009