Commission d’accès à l’information

Preventing confidentiality incidents

Checklist for private organizations

January 2026

Unofficial translation by BLG LLP

Source: Prévenir les incidents de confidentialité – Liste de contrôle pour les entreprises, CAI

Better safe than sorry!

You must limit the risks of a confidentiality incident within your organization by:

- complying with your obligations and the principles of personal information protection;
- implementing appropriate security measures;
- ensuring that these measures are applied at all times to guarantee their effectiveness.

The Commission offers this practical list to support you at each stage of the process set out in its document *Preventing confidentiality incidents – Practical guide for private organizations* [also unofficially translated by BLG].

This tool is a model that must be adapted to your organization's context. Its purpose is to guide reflection on the prevention of confidentiality incidents. Checking the boxes in this document does not ensure that your actions are compliant.

Step 1
Know and comply with your obligations

Complying with your obligations helps prevent confidentiality incidents or minimize their impacts.

Below is a list of the most important obligations relating to the protection of personal information. However, other obligations also apply. To learn more, consult the Personal information protection – Businesses and private organizations section on the Commission's website (available in French only).

With respect to collection

*Get a head start by collecting only the personal information that is **necessary**!*

- ☐ You have determined the purposes of the collection, and have concluded that you have a serious and legitimate interest in collecting personal information about your staff or your clientele.
- ☐ You are collecting only the personal information that is necessary (for example, to hire staff and manage employee files, or to offer your goods or services).

Remember: personal information that your organization has not collected cannot be involved in a confidentiality incident!

- ☐ Your collection is carried out by lawful means (that is, legal and legitimate means).
- ☐ When collecting information concerning your staff or your clientele, you have at least informed them of:

- ☐ the purposes of the collection;
- ☐ the means used to carry out the collection;
- ☐ their rights of access and rectification;
- ☐ their right to withdraw their consent to the communication or use of the information collected.

Remember: an individual who is informed of their rights is twice as vigilant! They will be much more attentive to the protection of their personal information and more alert in the event of an incident if they know, for example, which categories of persons or third parties may use or hold their information. You must provide this information upon request, but you may also incorporate it into your privacy policy.

- ☐ You have obtained valid consent (available in French only) from the individuals concerned before collecting their personal information from a third party, unless an exception applies under the *Act respecting the Protection of personal information in the private sector* (Private Sector Act).
- ☐ You have planned for a periodic review of the various collections of personal information relating to your staff and your clientele.

For more information, please consult:

- Collection of personal information (available in French only)
- Identity documents (available in French only)

With respect to the use

As a basic principle, only personal information that is necessary must be used!

- ☐ You are granting access to personal information only to staff members when such information is necessary for the performance of their duties.

Remember: staff members with restricted access rights cannot compromise all of the information held by your organization!

- ☐ Once the purposes have been fulfilled, you are limiting the use of personal information to the purposes to which the individuals concerned have consented or that are permitted by law.

With respect to communication

Communicate only what is authorized, in a secure manner!

- ☐ You have obtained the consent of the individuals concerned (available in French only) to disclose their personal information to a third party (for example, an insurer or a service provider), unless an exception applies under the Private Sector Act.
- ☐ You and your staff are making sure that personal information disclosed outside Québec, or processed on your behalf by a person or organization outside Québec, is afforded a level of protection equivalent to that provided by generally recognized personal information protection principles. You demonstrate this protection through a privacy impact assessment [as detailed in BLG's unofficial translation].
  - ☐ You have also entered into an agreement with the person or organization receiving this information.
- ☐ You have entered into written agreements to govern the disclosure of personal information to a service provider as part of a mandate, or for the performance of a service or enterprise contract.

With respect to retention and destruction

Keep only accurate and up-to-date information, and not forever!

- ☐ The personal information you hold about your staff and your clientele is accurate and up to date at the time it is used.
- ☐ As soon as the purpose for which the personal information was collected or used has been fulfilled, you dispose of it by:
  - ☐ destroying it in a secure manner, subject to the retention period provided for by law (for example, for tax obligations);
  - ☐ anonymizing it (available in French only) in order to use it for serious and legitimate purposes.

Remember: personal information that your organization has destroyed cannot be compromised!

For more information, please consult:

- Retention and destruction of personal information (available in French only)

Step 2
Inventory personal information that is held and assess its sensitivity

Understanding the information you hold will help you protect it better!

- ☐ You have carried out an inventory of the personal information held by your organization. This inventory specifies:
  - ☐ The types of personal information your organization collects about its clientele or staff (for example, credit card number, address, telephone number);
  - ☐ The scope of the information;
  - ☐ The purposes (objective sought, expected outcome) for which it is necessary for your organization to collect this personal information;
  - ☐ An assessment of the degree of sensitivity of this information;
  - ☐ The manner in which your organization collects this information;
  - ☐ The categories of persons authorized to have access to it within the organization or externally (third parties);
  - ☐ The context in which this information is used or communicated within or outside the organization, or the manner in which it is used or communicated;
  - ☐ The location and jurisdiction where this information is stored, the media on which it is stored, and the conditions under which it is stored;
  - ☐ The manner in which your organization disposes of this information once the purpose justifying its collection has been fulfilled.

To structure your inventory, please consult [BLG's unofficial translation of] Conducting a privacy impact assessment.

Step 3
Identify the risks and assess the consequences

Failing to assess your risks is an even greater risk!

- ☐ You have identified the situations or events (risks) that could reasonably occur and threaten the personal information held by your organization (for example, theft or unauthorized communication).

- ☐ You have analyzed the causes likely to give rise to these risks (for example, insufficient or non-existent verification mechanisms, lack of knowledge or training, errors in handling information).
- ☐ You have assessed the potential impact of each risk (for example, very low or none, low, high, very high).
- ☐ You have estimated the likelihood that these risks will materialize.
- ☐ You have considered existing strategies and security measures.
- ☐ You have determined the tolerance threshold for each risk.

Step 4
Determine the appropriate measures

Adopting appropriate security measures: a first step toward well-protected personal information!

- ☐ You have implemented your legal obligation to designate a person responsible for the protection of personal information within your organization.
- ☐ As required by law, your organization has adopted policies and practices guiding its governance of the personal information it holds. For example:
  - ☐ Your organization regularly provides its staff with training and awareness sessions on the protection of personal information, and the policies and practices in force.
  - ☐ Your organization has adopted a policy, guidelines, or procedures regarding the use of personal mobile devices in the workplace or the use of work-issued mobile devices outside the workplace.
  - ☐ In the case of contracts entered into with third parties such as service providers or suppliers, your organization has adopted policies, procedures, or guidelines establishing personal information protection requirements.
  - ☐ You have verified the security measures implemented by third parties with whom you share personal information.
- ☐ Your organization has adopted technical security measures to protect the personal information it holds. For example:

- ☐ Procedures to guide staff on the applicable measures to secure networks (including wireless networks), prevent malware attacks, manage user access, etc.
- ☐ Practices that promote the prevention of confidentiality incidents, such as strong passwords, encryption of communications, firewalls, data de-identification, software updates, etc.

☐ Your organization has adopted physical security measures to ensure the protection of the personal information it holds (for example, locked premises and filing cabinets, restricted access, etc.).

☐ Your organization has adopted other policies, procedures, or guidelines that may have a positive impact on the prevention of confidentiality incidents.

Step 5
Implement the security measures

Plan the implementation of your measures, and ensure their full and integrated implementation!

☐ Through its actions, senior management demonstrates that the protection of personal information is an organizational priority and that it is fulfilling its legal obligation to ensure such protection.

☐ In doing so, it exercises strong and mobilizing leadership by:

- ☐ Approving the security measures implemented and ensuring their oversight;
- ☐ Actively promoting them among staff;
- ☐ Providing the necessary resources to ensure the implementation and maintenance of a strong culture of personal information protection.

☐ You have developed an action plan in collaboration with the persons who will be responsible for its implementation.

☐ You have developed a communication strategy to inform your staff of the measures.

☐ The measures implemented are clear, comprehensive, concrete, and consistent.

Step 6
Measure the effectiveness of the measures

Assess the effectiveness of your measures!

- ☐ You have measured the performance of the security strategies and measures you have implemented using measurement tools (for example, phishing exercises conducted with staff before and after an awareness campaign), or other sources of feedback (for example, analysis of complaints received regarding personal information protection practices).
- ☐ You have reassessed the level of each risk in light of the measures deployed.

Step 7
Monitor the implementation of these measures and review them

Protecting personal information is not a one-day effort!

- ☐ You have put mechanisms in place to actively monitor the effectiveness of the security measures deployed.
- ☐ You regularly reassess the effectiveness of these measures and update them.
- ☐ Your organization has adopted a policy, guidelines, or procedures for the management of confidentiality incidents (for example, procedures to detect, document, or report incidents and respond to them, including measures to mitigate the risks associated with such incidents, and prevention strategies to prevent their recurrence). Moreover, every organization must keep a register in which it records all confidentiality incidents involving personal information.

Did you find this information tool helpful? Complete [the CAI's] short satisfaction survey (available in French only)!