Commission d’accès à l’information

Preventing confidentiality incidents

Practical guide for private organizations

January 2026

Unofficial translation by BLG LLP

Source: Prévenir les incidents de confidentialité - Guide explicatif pour les entreprises, CAI

Better safe than sorry!

Your organization has an obligation to implement appropriate security measures to protect personal information.[1]

By doing so, you help promote the privacy of your clients and employees, and reduce the risk of harm to your reputation.

This guide aims to answer the following questions:

- **What is a confidentiality incident?**
- **How do you distinguish between the protection of personal information and IT security?**
- **How do you protect personal information?**

In addition to this practical guide, the Commission renders available another document, *Preventing confidentiality incidents — Checklist for organizations* [also unofficially translated by BLG]. This handy tool is designed to help organizations ask themselves the right questions as part of their prevention efforts.

[1] This obligation is provided for in Section 10 of the *Act respecting the protection of personal information in the private sector*.

Table of contents

What is a confidentiality incident?

A confidentiality incident occurs when personal information is accessed, used, or communicated without legal authorization, or when such information is lost or stolen.

This type of incident can take several forms:

- Unauthorized access, extraction, or communication of personal information
- Sending a communication to the wrong person
- Communicating personal information through gossip inside or outside the workplace (for example, on the bus)
- Data loss caused by a virus, an IT vulnerability, or human error
- Security breach resulting from a cyberattack (for example, phishing or ransomware)
- Unauthorized third-party intrusion into the IT system

Which organizations are concerned?

Every organization is at risk of experiencing a confidentiality incident. Whether you are the holder of personal information or a service provider, you must implement concrete measures to protect personal information and regularly assess their effectiveness to keep them up to date. Otherwise, the likelihood that your organization will be affected by an incident is higher.

What are the consequences?

A confidentiality incident puts at risk the privacy of the individuals concerned. These may be your clients, your staff, or your business partners.

The potential consequences can be significant, and a person's life can be profoundly affected following an incident. They may, for example, become a victim of identity theft or fraud, experience discrimination, suffer severe psychological distress, or even—in some cases—see their physical safety threatened.

You therefore have a duty toward the individuals whose personal information you hold to minimize the risk that they will be affected by a confidentiality incident, thereby also reducing risks for your organization. Indeed, such an incident may undermine public trust in your organization by damaging its reputation. It may also affect profitability, as responding to the incident can generate significant costs and negatively impact your revenue.

What are the causes?

There are different types of threats to the confidentiality of personal information. They may be:

- **Human**: phishing, hacking, indiscretions, loss or theft of personal information by an employee, accidental communication, etc.
- **Technological**: absence of a firewall, outdated software, unencrypted data, services that are unsecured or retained even though they are no longer needed, etc.
- **Physical**: for example, accessibility of the server room or of the premises where documents containing personal information are stored.

Personal information protection and IT security

The protection of personal information and IT security are complementary, but they are not synonymous. Effective security measures are only one of the important principles of personal information protection, which also depends on sound governance, transparency, limiting collection, etc.

In short, IT security measures contribute to the protection of personal information, but they do not automatically prevent intrusions into individuals' privacy.

Here are examples where a good security measure nevertheless raises issues of non-compliance with the law and with personal information protection principles:

Non-compliant collection

You configure a form to allow for the secure collection of personal information, but the information is not necessary for processing the client's file, or for providing your goods or services.

Non-compliant use

You store personal information in a highly secure system, but you use it for purposes other than those for which it was collected or to which the client consented, and that are not authorized by law.

Non-compliant communication

You secure an electronic communication to preserve the confidentiality of its content, but you send it to a person who is not authorized to access the personal information it contains.

Non-compliant retention

You encrypt the personal information you hold and restrict access to it, but it is not up to date or accurate when you use it to make a decision about the individual concerned, or you retain it when it should have been destroyed.

How to protect personal information?

Under Section 10 of the *Act respecting the protection of personal information in the private sector*, “a person carrying on an enterprise must take the security measures necessary to ensure the protection of the personal information collected, used, communicated, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored.”

To support you in implementing this obligation, the Commission proposes a **seven-step** process to prevent confidentiality incidents or mitigate their consequences.

Step 1
Know and comply with your personal information protection obligations

You must know and comply with your obligations regarding the protection of personal information. By doing so, your organization will be less likely to be affected by a confidentiality incident.

For example, if staff members have restricted access rights, they cannot compromise all the personal information held by your organization. Likewise, hackers cannot steal personal information that your organization does not hold because it was never collected or was destroyed.

To learn more, consult the Protection of personal information — Private-sector organizations section (available in French only) on the Commission's website.

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

It is essential to take inventory of the personal information held by your organization.[2] You must document, in particular, its sensitivity, its purpose (what it is used for), its quantity, its distribution, and the medium on which it is stored, as well as its lifecycle within your organization—from collection to destruction. You must also know who has access to it and in what context it is used.

To structure your inventory, ask yourself the following questions:

- What types of personal information does your organization collect about its clients or its personnel?
- What is the scope of the information involved?
- What is the nature of this information? Is it sensitive due to its nature (medical, biometric, or otherwise intimate), or due to the context in which it is used?
- Why and how is this information collected, used, communicated, or retained? What is its purpose?
- Which categories of individuals may have access to it within or outside your organization (third parties)?
- How many people will have access to the information, and why do they need it to perform their duties?
- How do the individuals who have access to the information use or communicate it?
- Where is this information retained? On which media and under what conditions?
- How do you destroy this information once the purpose of its collection has been achieved?

[2] For more information about the steps to follow to inventory personal information, consult [BLG's unofficial translation of] Conducting a Privacy Impact Assessment (PIA).

- If the information is anonymized for serious and legitimate purposes, is it anonymized according to generally recognized best practices and in a manner consistent with the *Regulation respecting the anonymization of personal information*?

Here is a template table designed to help you conduct this exercise:

Questions	What you have to do
What?	Enter the type of personal information collected (for example, address, date of birth, etc.), the amount of information, and the sensitivity of the information
Why?	List the reasons why it is necessary for your organization to collect this personal information
Who?	List the categories of persons authorized to have access to this information within or outside the company, and why it is necessary for the performance of their duties
How?	Indicate the context or manner in which this information is used or communicated within or outside the company
Where?	Indicate where this information is stored within or outside the company and on what types of media
When?	Indicate when this information must be destroyed and the secure destruction method used

An inventory of the personal information held by your organization allows you to better anticipate the measures needed to protect it. These measures must be reasonable given the sensitivity of the information, the purposes for which it is used, its quantity, its distribution, and the medium on which it is stored.

This inventory exercise is also useful for assessing the compliance of your practices regarding the protection of personal information, particularly if you are launching a project that requires a privacy impact assessment [as detailed in BLG's unofficial translation].

Assessing the context in which the information is processed

The extent of the security measures must be proportionate to the context: they must be adapted to the sensitivity of the personal information, the purposes for which it is used, its quantity, its distribution, and the medium on which it is stored. At this stage, you should reflect on each of these factors to make it easier to determine which measures to adopt later (see step 4).

Sensitivity

Personal information is sensitive when it gives rise to a high degree of reasonable expectation of privacy, due to its nature or the context in which it is used or communicated. Section 12 of the *Act respecting the protection of personal information in the private sector* specifies, for example, that medical or biometric information is sensitive by nature, but any type of information may be considered sensitive in a given context.

For example, information may be considered sensitive if it is used in a project involving a vulnerable population (for example, minors, ethnocultural minorities, sexual minorities).

Purpose

For what purposes is the personal information used or communicated? Are these purposes generally risky for individuals? Do they produce significant effects (for example, legal effects) on them? If, despite the purpose for collecting the personal information, the risks are too high, the organization must reassess the necessity criterion (available in French only) for the collection, as its proportionality may be compromised.

Quantity

How much personal information is involved? Does quantity influence the magnitude of the foreseeable risks?

The more sensitive personal information an organization holds (for example, social insurance number, credit card number, medical information) and the more its management context exposes it to risks (for example, use by several people, distribution across different media, communication to third parties), the more robust the security measures must be.

Distribution

How is the personal information distributed? Are the physical locations where it is retained secure and adequately protected? To whom is it communicated? How many people have access to the information, and across how many media is it hosted?

Do the cloud servers used offer security guarantees that meet industry standards? Are the rules applicable in the country where the cloud servers are located sufficient to protect the information as if it were hosted in Québec?

Media

What types of storage media allow for the consultation or recording—or both—of personal information, whether temporarily or long-term? Is it a physical or digital medium, or both? Is this medium secure? Is it connected to other systems?

In short, security measures must be proportionate to the sensitivity of the personal information, as well as to its purpose, its quantity, its distribution, and the medium on which it is stored.

To learn more about how to assess these elements when taking inventory of the personal information you hold, consult [BLG's unofficial translation of] Conducting a privacy impact assessment.

Step 3
Identify the risks and assess the consequences

After taking inventory of the personal information held by your organization and documenting its context, you must identify the risks (events) that could threaten it.

You will then be able to analyze the potential causes of the identified risks, assess the consequences of a confidentiality incident for the individuals concerned, and estimate the likelihood that these risks will occur.

Here are some examples:

- **Risks:**
    - Theft of personal information;
    - Loss or unauthorized communication;
    - Re-identification of depersonalized or anonymized personal information;
    - Retention of information when its usefulness can no longer be demonstrated
- **Potential causes:**
    - Lack of staff knowledge or training;
    - Inadequate management of access to personal information;
    - Absence of a data retention and destruction policy (or lack of awareness of this policy)
- **Potential consequences in case of a confidentiality incident:**
    - Unwanted solicitation;
    - Identity theft and fraud;
    - Psychological distress, discrimination, harassment, manipulation.

A consequence may be visible and external (for example, harm to reputation) or experienced internally by the affected individuals (for example, a feeling of intrusion).

For more information on risk and consequence assessment, consult [BLG's unofficial translation of] Conducting a privacy impact assessment.

Step 4
Determine the appropriate measures

In light of the risk analysis and the assessment of their consequences, you can determine which security measures you must implement to mitigate the risks. If your organization already has risk mitigation measures in place, you must assess their effectiveness and adjust them as needed.

Below are examples of security measures that can help protect personal information within an organization. **The items in bold are obligations set out in the law**.

Administrative or organizational measures

Governance measures

- **Ensure that policies and practices relating to the protection of personal information are up to date** (for example, data retention and destruction policy, contract management processes that take personal information protection into account);
- Establish an information security and privacy committee that brings together individuals who play a strategic role within your organization and report to senior management;
- Clearly communicate your expectations to staff;
- Report periodically to senior management.

Tactical measures

- **Train and raise awareness among staff** (for example, strong passwords, risks related to malware or social engineering, or clean-desk principles);
- **Develop an annual action plan** for adding new security measures;
- Actively monitor the effectiveness of the measures in place.

Operational measures

- Grant access rights to personal information only to staff whose duties require such access;
- **Depending on the size of your organization, designate representatives** who can advise their colleagues on the identified security measures;
- **Develop standard templates** (for example, personal information collection form, confidentiality undertaking, non-disclosure agreement, contracts) **and review them periodically**;
- Use a robust identification protocol

Physical measures

- Control access (for example, offices, server rooms, wiring rooms, alarm systems);
- Restrict access to premises or filing cabinets where paper documents containing personal information are stored.

Technical measures

- Promote strong usernames and passwords;
- Ensure the encryption of communications and stored information;
- Encrypt mobile devices;
- Implement a firewall;
- Ensure perimeter network defence;

- Depersonalize information before use when individuals' identities are not required for the intended processing;
- Ensure effective management of employee access to personal information, keep logs of such access, and analyze the logs to detect irregular situations;
- Systematically apply software updates;
- Block USB ports;
- Adopt a document-management system;
- Implement methods that allow for the secure destruction of personal information.

Step 5
Implement the security measures

After determining the measures to implement to reduce the identified risks, you must plan their complete and integrated deployment. To support this process, develop an action plan and a communication strategy.

The 10 Cs: Making sure nothing is overlooked!

Consultation and communication: Two prerequisites for effective change management

Are you planning to implement or enhance security measures? Consulting with the individuals who will be responsible for implementing them will help you ensure that the proposed measures make sense in their day-to-day reality.

Staff members may provide information about their work context that could lead you to adjust certain strategies or measures.

Good communication will also help ensure that these individuals understand your objectives, buy into them, and apply the measures in line with your expectations.

Complete, clear, concrete and coherent

Ensure that you implement complete and integrated measures, drafted in clear terms, and that are concrete and coherent so that they are well understood and applied by all staff members.

Consistency, control and consequences

Protecting personal information is not a one-day effort. The effectiveness of your measures will depend on their consistency and the control you implement to ensure they are followed.

For example, you could implement mechanisms to control access to personal information and maintain access logs, allowing you to know who accessed which information. You should also inform the relevant staff members of the monitoring and control measures that apply to them.

Finally, staff should also be informed of the consequences (for example, disciplinary measures) they may face if they act indiscreetly, fail to follow policies and directives, or breach security measures.

Step 6
Measure the effectiveness of the measures

At this stage, you should measure the performance of the strategies and measures you have implemented. For example, if you conducted an awareness campaign on phishing risks for staff, assess its impact to determine whether improvements are required.

Various tools can help you evaluate the effectiveness of your measures:

- Satisfaction surveys;
- Log analysis;
- Behavioural reports;
- Intrusion and vulnerability tests.

Evaluation and feedback will provide you with additional information to help you assess the level of risk following the application of the measures. You can then determine whether this new threshold is acceptable and strengthen the measures already in place.

Step 7
Monitor the implementation of these measures and review them

To ensure the effectiveness of your security measures, you must monitor their application and revise them in light of emerging risks. Your measures must also adapt to changes within your organization, such as a new line of business, a new transactional system, or a new information-sharing tool.

Control tools, such as a security dashboard, will allow you to maintain an overview of the consistent and integrated application of the strategies and measures you have implemented.

Here are examples of questions you may wish to consider:

- Are your processes for granting and managing IT access reviewed regularly? For instance, are access cards and access codes for individuals leaving the building deactivated in a timely manner?
- Do you regularly audit your staff's practices regarding the protection of personal information (for example, through malware simulations or mystery client exercises)?

Better safe than sorry!

Would you know how to react if a confidentiality incident occurred within your organization? An incident response plan will help you act more quickly and effectively, limit the consequences of the incident, support proper remediation of the affected systems, and resume your operations promptly.

What should you do in the event of a confidentiality incident?

It is very likely (if not certain) that your organization will eventually experience a confidentiality incident, whether minor or significant in scope. You will then need to react quickly to limit risks, assess potential harm, and, in some cases, notify the Commission and the affected individuals.

If you have reasonable grounds to believe that a confidentiality incident has occurred within your organization, you must take reasonable measures to reduce the risk of harm and prevent similar incidents from happening again.

In addition, for every confidentiality incident, you must assess the severity of the risk of injury to the affected individuals. If your analysis shows a risk of serious injury, you must notify the Commission and the affected individuals.

You must also keep a log and record all confidentiality incidents, whether or not the risk of injury is serious.

For more information, consult the page Confidentiality incidents and security measures (available in French only).

Reminders

To be effective, your security measures must take several elements into account, such as the sensitivity of the information, the purpose of their use, their quantity, how they are used, how they are distributed, and their storage format.

These measures must be implemented, communicated to all staff, documented, monitored, and reviewed regularly.

Have security measures aimed at protecting personal information been implemented within your organization? Are you confident in the effectiveness of these measures?

To help you apply the risk management approach proposed in this guide, consult [BLG's unofficial translation of] the practical tool *Preventing confidentiality incidents – Checklist for organizations.*

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