Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

PRIVACY BREACH CHECKLIST

For more details, please see *Key Steps for Organizations in Responding to Privacy Breaches*.

Incident Description

- What was the date of the incident?
- When was the incident discovered?
- How was it discovered?
- What was the location of the incident?
- What was the cause of the incident?

Step 1: Breach Containment and Preliminary Assessment

- Have you contained the breach (recovery of information, computer system shut down, locks changed)?
- Have you designated an appropriate individual to lead the initial investigation?
- Is there a need to assemble a breach response team? If so, who should be included (e.g., privacy officer, security officer, communications, risk management, legal)?
- Have you determined who needs to be made aware of the incident internally and potentially externally at this preliminary stage?
- Does the breach appear to involve theft or other criminal activity? If yes, have the police been notified?
- Have you made sure that evidence that may be necessary to investigate the breach has not been destroyed?

Step 2: Evaluate the Risks Associated with the Breach

(i) What personal information was involved?

- What personal information was involved (name, address, SIN, financial, medical)?
- What form was it in (e.g., paper records, electronic database)?
- What physical or technical security measures were in place at the time of the incident (locks, alarm systems, encryption, passwords, etc.)?

(ii) What was the cause and extent of the breach?

- Is there a risk of ongoing breaches or further exposure of the information?
- Can the personal information be used for fraudulent or other purposes?
- Was the information lost or was it stolen? If it was stolen, can it be determined whether the information was the target of the theft or not?
- Has the personal information been recovered?
- Is this a systemic problem or an isolated incident?

(iii) How many individuals have been affected by the breach and who are they (e.g., employees, contractors, public, clients, service providers, other organizations)?

(iv) Is there any foreseeable harm from the breach?

- What harm to the individuals could result from the breach(e.g., security risk, identity theft, financial loss, loss of business or employment opportunities, physical harm, humiliation, damage to reputation, etc.)?

- Do you know who has received the information and what is the risk of further access, use or disclosure?
- What harm to the organization could result from the breach (e.g., loss of trust, loss of assets, financial exposure, legal proceedings, etc.)
- What harm could come to the public as a result of notification of the breach (e.g., risk to public health or risk to public safety)?

Step 3: Notification

(i) Should affected individuals be notified?

- What are the reasonable expectations of the individuals concerned?
- What is the risk of harm to the individual? Is there a reasonable risk of identity theft or fraud?
- Is there a risk of physical harm? Is there a risk of humiliation or damage to the individual's reputation?
- What is the ability of the individual to avoid or mitigate possible harm?
- What are the legal and contractual obligations of the organization?

If you decide that affected individuals do not need to be notified, note your reasons.

(ii) If affected individuals are to be notified, when and, how will they be notified and who will notify them?

- What form of notification will you use (e.g., by phone, letter, email or in person, website, media, etc.)?
- Who will notify the affected individuals? Do you need to involve another party?
- If law enforcement authorities are involved, does notification need to be delayed to ensure that the investigation is not compromised?

(iii) What should be included in the notification?

Depending on the circumstances, notifications could include some of the following, but be careful to limit the amount of personal information disclosed in the notification to what is necessary:

- information about the incident and its timing in general terms;
- a description of the personal information involved in the breach;
- a general account of what your organization has done to control or reduce the harm;
- what your organization will do to assist individuals and steps individuals can take to reduce the risk of harm or further protect themselves;
- sources of information designed to assist individuals in protecting against identity theft;
- contact information of a department or individual within your organization who can answer questions or provide further information;
- whether your organization has notified a privacy commissioner's office;
- additional contact information to address any privacy concerns to your organization; and
- contact information for the appropriate privacy commissioner(s).

(iv) Are there others who should be informed about the breach?

- Should any privacy commissioners' office be informed? [Insert link?]
- Should the police or any other parties be informed? This may include insurers; professional or other regulatory bodies; credit card companies, financial institutions or credit reporting agencies; other internal or external parties such as third party contractors, internal business units not previously advised of the privacy breach, union or other employee bargaining units)

Step 4: Prevention of Future Breaches

- What short or long-term steps do you need to take to correct the situation (e.g., staff training, policy review or development, audit)?