Privacy Breach Checklist for Public Bodies

Use this form to evaluate your public body's response to a privacy breach. The form can also be submitted to the OIPC for the purpose of mandatory notification, as it includes fields for all of the information required under the *Freedom of Information and Protection of Privacy Act*. If you are reporting the breach to the OIPC through the checklist or the online form, you must answer all of the questions. If a question does not apply to your situation, write "N/A." If you do not know the answer, write "unknown." Completed forms can be emailed to info@oipc.bc.ca

The preferred method for public bodies to report privacy breaches is by using our online form: https://www.oipc.bc.ca/forms/public-bodies/online-privacy-breach-report-form/

Information entered into the online form is secured through encryption in transit and storage.

For more information on reporting a privacy breach, visit:
https://www.oipc.bc.ca/resources/report-a-privacy-breach/

Contact information

Public Body:

Contact Person:

Name:

Preferred pronoun:

Title:

Phone:

Email:

Mailing address:

Risk evaluation

Incident Description

1. Describe the breach and its cause:

2. Date of the breach or period when it occurred:

3. Date breach discovered:

4. Location of breach:

5. Estimated number of individuals affected:

6. Type of individuals affected:

- ☐ Client/Customer/Patient
- ☐ Employee
- ☐ Student
- ☐ Other:

Personal Information Involved

7. Describe the personal information involved (e.g. name, address, SIN, financial, medical): (Do not include or send us identifiable personal information)

Safeguards

8. Describe physical security measures (locks, alarm systems etc.):

9. Describe technical security measures:

- ☐ Encryption
- ☐ Password
- ☐ Other (Describe):

Describe organizational security measures (security clearances, policies, role-based access, training programs, contractual provisions):

Harm from the Breach

10. Identify the type of harm(s) that may result from the breach:

- ☐ Identity theft (most likely when the breach includes loss of SIN, credit card numbers, driver's licence numbers, personal health numbers, debit card numbers with password information and any other information that can be used to commit financial fraud) or significant:
  - ☐ Bodily harm (when the loss of information places any individual at risk of physical harm, stalking or harassment);
  - ☐ Humiliation (associated with the loss of information such as medical records, disciplinary records);
  - ☐ Damage to reputation or relationships;
  - ☐ Loss of employment, business or professional opportunities (usually as a result of damage to reputation to an individual);
  - ☐ Financial loss;
  - ☐ Negative impact on a credit record, or;
  - ☐ Damage to, or loss of, property;
- ☐ Breach of contractual obligations;
- ☐ Future breaches due to similar technical failures;
- ☐ Failure to meet professional or certification standards;
- ☐ Other (specify): ☐

Notification

11. Has your Privacy Officer been notified?

☐ Yes Who was notified and when? _____

☐ No When to be notified? _____

12. Have the police or other authorities been notified (e.g. professional bodies or persons required under contract)?

☐ Yes Who was notified and when? _____

☐ No When to be notified? _____

13. Have affected individuals been notified?

☐ Yes Manner of notification: _____
Number of individuals notified: _____
Date of notification: _____

☐ No Why not? _____

14. What information was included in the notification?

☐ The name of the public body;

☐ The date on which the privacy breach came to the attention of the public body;

☐ A description of the privacy breach including, if known,

- ☐ (a) the date on which or the period during which the privacy breach occurred, and;
- ☐ (b) a description of the nature of the personal information involved in the privacy breach;

☐ Confirmation that the Commissioner has been or will be notified of the privacy breach;

- ☐ Contact information for a person who can answer, on behalf of the public body, questions about the privacy breach;

- ☐ A description of steps, if any, that the public body has taken or will take to reduce the risk of harm to the affected individual;

- ☐ A description of steps, if any, that the affected individual could take to reduce the risk of harm that could result from the privacy breach.

Notifying the OIPC

15. The Office of the Information and Privacy Commissioner must be notified of the breach if the breach could reasonably be expected to result in significant harm to the individual, including any of the harms listed below:

- ☐ Identity theft or significant
    - ☐ Bodily harm;
    - ☐ Humiliation;
    - ☐ Damage to reputation or relationships;
    - ☐ Loss of employment, business or professional opportunities;
    - ☐ Financial loss;
    - ☐ Negative impact on a credit record, or;
    - ☐ Damage to, or loss of, property

16. If you are reporting the breach to the OIPC, you must include the following information (note: there are fields in this checklist and in the online form that address each of the factors listed below):

- ☐ The name of the public body;
- ☐ The date on which the privacy breach came to the attention of the public body;
- ☐ A description of the privacy breach including, if known,
  - ☐ the date on which or the period during which the privacy breach occurred;
  - ☐ a description of the nature of the personal information involved in the privacy breach; and
  - ☐ an estimate of the number of affected individuals;
- ☐ Contact information for a person who can answer, on behalf of the public body, questions about the privacy breach;
- ☐ A description of steps, if any, that the public body has taken or will take to reduce the risk of harm to the affected individuals.

Prevention

17. Describe the steps taken to contain and reduce the harm of the breach (e.g. locks changed, computer access codes changed or revoked, computer systems shut down):

18. Describe the long-term strategies you will take to correct the situation (e.g. staff training, policy development, privacy and security audit, contractor supervision strategies, improved technical security architecture, improved physical security):

If you have completed a security audit and are reporting this breach to the OIPC, please forward a copy of the audit with your report.