Yukon Information and Privacy Commissioner

Privacy Breach Checklist

Report Date:

Contact Information

1. Public Body: _____

2. Contact Person:

   Name: _____

   Title: _____

   Phone: _____ Fax: _____

   E-Mail: _____

   Mailing address: _____

   _____

Risk Evaluation

Incident Description

3. Describe the nature of the breach and its cause.

4. Date of incident: _____

5. Date incident discovered: _____

6. Location of incident: _____

7. Estimated number of individuals affected**:** _____

8. Type of individual(s) affected:

☐ Client / Customer / Patient

- ☐ Employee
- ☐ Student
- ☐ Other**:** _____

Personal Information Involved

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

Safeguards

10. Describe the physical security measures (locks, alarm systems etc.).

11. Describe the technical security measures:

    - ☐ Encryption
    - ☐ Password
    - ☐ Other, please describe.

12. Describe the public body's security measures (security clearances, policies, training programs, contractual provisions).

Harm from the Breach

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

- ❑ Identify theft
  (most likely when the breach includes loss of S.I.N., 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)
- ❑ Risk of physical harm
  (when the loss of information places any individual(s) at risk of physical harm, stalking or harassment)
- ❑ Hurt, humiliation, damage to reputation
  (associated with the loss of information such as mental health records, medical records, disciplinary records)
- ❑ Loss of business or employment opportunities
  (usually as a result of damage to reputation to an individual(s))
- ❑ Breach of contractual obligations
  (contractual provisions may require notification of third parties in the case of a data loss or privacy breach)
- ❑ Future breaches due to similar technical failures
  (notification to the manufacturer may be necessary if a recall is warranted and/or to prevent a future breach by other users)

- ❑ Failure to meet professional standards or certification standards
  (notification may be required to professional regulatory body or certification authority)

- ❑ Other, please specify.

Notification

14. Has the ATIPP Coordinator/ Director or Manager responsible for information and privacy issues 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: _____

    ☐ No Why not? _____

14. What information was included in the notification?
    - ❑ Date of the breach
    - ❑ Description of the breach
    - ❑ Description of the information inappropriately accessed, collected, used or disclosed
    - ❑ Risk(s) to the individual(s) caused by the breach
    - ❑ Steps taken so far to control or reduce the harm
    - ❑ Future steps planned to prevent further privacy breaches
    - ❑ Steps the individual(s) can take to reduce the harm
    - ❑ IPC contact information
    - ❑ Organization contact information for further assistance

15. Was the IPC notified? Consider the following factors:
    - ❑ The personal information involved is sensitive
    - ❑ There is a risk of identity theft or other harm including pain and suffering or loss of reputation
    - ❑ A large number of people or affected by the breach
    - ❑ The information has not been fully recovered
    - ❑ The breach is the result of a systemic problem or a similar breach has occurred before

- ❑ The public body requires assistance in responding to the privacy breach
- ❑ The public body wants ensure that the steps taken comply with the public body's obligations under privacy legislation

Please include a copy of the notification letter(s) if applicable.

Mitigation and Prevention

16. Describe the immediate 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).

17. 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).

NOTE: Reporting a privacy breach to the IPC does not preclude the IPC from reviewing the incident upon referral.