|  |
| --- |
| **Privacy Breach Internal Investigation Report Guide for Public Bodies** |

This document is to outline the essential information that should be included in a public body and/or trustee’s internal investigation of a privacy breach. If you are submitting an internal investigation report to the IPC, please include supporting documents such as relevant policies, procedures, and copies of notification letters.

|  |
| --- |
| Public Body/Trustee Contact information |

Even after providing an internal investigation report to the IPC, we may need to contact the public body/trustee to ask questions so we can fully understand the situation. Please provide the name of an employee who the IPC can work with in resolving matters regarding the privacy breach.

1. Name:
2. Position Title:
3. Telephone Number:
4. Email Address:

|  |
| --- |
| Initial steps in containing the privacy breach |

Soon after a public body/trustee learns of a privacy breach, it should contain and recover any personal information/personal health information that is involved. This will require determining how broad the privacy breach is. If paper records are involved, then efforts should be made to physically recover the paper records. If electronic records are involved, then efforts should be made:

* To physically recover any devices that contain information, such as USB key, CDs, and DVDs;
* to recall emails and/or requesting recipients to destroy the email contain personal information/personal health information;
* to immediately take down personal information/personal information if it was posted online.

In some cases, the privacy breach can be ongoing. For example, an employee continues to snoop. In such cases, the public body/trustee should prevent the employee from accessing personal information/personal health information. In other cases, devices such as laptops containing personal information/personal health information, could have been stolen. In such cases, the police should be contacted.

Please provide responses to the following questions:

1. What efforts have the public body/trustee made to contain the privacy breach?
2. Has the privacy breach been contained completely? Why or why not?

|  |
| --- |
| Details of the privacy breach |

Please provide a description of the privacy breach. Details should include the following:

1. When did the privacy breach occur?
2. When did the public body/trustee learn of the breach (if different from above)?
3. What happened? Please describe the circumstances that contributed to the privacy breach.
4. Which employee(s) are involved or witnessed the privacy breach?
5. How did the public body/trustee learn of the privacy breach?
6. What type of personal information/personal health information is involved? Examples of personal information/personal health information include individuals' names, contact information, financial information, medical information.

|  |
| --- |
| Assessment of Risks to Affected Individuals |

The person to whom the information involved in the breach is the affected individual. There can be more than one affected individual in a privacy breach.

1. How many individuals are affected?
2. Has the public body identified the risks that the affected individuals will be exposed to because of the privacy breach? Risks can be harm to physical safety, identity theft or fraud, hurt or humiliation, loss of trust in the public body/trustee or risk to public health or public safety.
3. Has the public body (or will the public body) notify the affected individuals? Why or why not? If notification was sent by letter, please provide our office with a copy.

|  |
| --- |
| Steps taken to prevent a similar privacy breach |

Public bodies/trustees should be safeguarding personal information/personal health information. Administrative, physical, and technical safeguards should be reviewed regularly to determine their adequacy in protecting information. They should also be reviewed after the discovery of a privacy breach has occurred.

Examples of **administrative safeguards** include policies, procedures, agreements, contracts, training resources. Examples of **physical safeguards** include locked filing cabinets, restricted access to areas containing personal information/personal health information, computer monitor privacy screens, and alarm systems. Examples of **technical safeguards** include protecting information through strong passwords and encryption, automatic log off features for computers (after a short time of user inactivity), and firewalls.

1. What administrative safeguards has the public body identified as relevant to this privacy breach? Please provide our office with copies.

2. What physical safeguards has the public body identified as relevant to this privacy breach?

3. What technical safeguards has the public body identified as relevant to this privacy breach?

4. Has the public body made changes to any of the identified safeguards to prevent similar privacy breaches?

5. Has the public body created any new safeguards to prevent similar privacy breaches? If so, please describe.