Guide to Creating an Internal Privacy Breach Investigation Report

This document assists public bodies and/or trustees in creating an internal privacy breach investigation report. It presents a series of questions that public bodies and/or trustees can use to assist them in investigating privacy breaches and preparing a privacy breach report.

Office of the
Saskatchewan Information
and Privacy Commissioner

Guide to Creating an Internal Privacy Breach Investigation Report

PURPOSE

The Office of the Information and Privacy Commissioner (OIPC) recommends the following five steps when a public body or trustee is responding to a privacy breach:

- contain the breach,
- notify affected individuals
- investigate the breach,
- prevent future breaches, and
- write a privacy breach report.

This document focuses on the last step of responding to a privacy breach, which is to write a privacy breach report. When the OIPC conducts an investigation into a privacy breach, it will ask the public body or trustee to submit an internal privacy breach investigation report. This document is to assist public bodies and trustees in creating its internal privacy breach investigation report. It presents a series of questions that public bodies and/or trustees can use to assist them in investigating privacy breaches and preparing a privacy breach report. Please note that it is not an exhaustive list of questions.

While the OIPC encourages public bodies and trustees to use this document as a guide, the OIPC does not require public bodies and trustees to submit its internal privacy breach investigation report in the format presented in this document. This document is meant only as a guide.

For additional guidance on how to manage privacy breaches, please refer to the following two resources:

1) *Privacy Breach Guidelines for Government Institutions and Local Authorities* at https://oipc.sk.ca/assets/privacy-breach-guidelines-for-government-institutions-and-local-authorities.pdf

2) *Privacy Breach Guidelines for Trustees* at https://oipc.sk.ca/assets/privacy-breach-guidelines-for-trustees.pdf

Public Body/Trustee Contact Information

Please provide the name of an employee who the IPC can work with in resolving matters regarding the privacy breach.

Employee	Telephone	Email	Office Location & Hours
[Employee name and title]	[Telephone number]	[Email address]	[Location, Hours, Days]

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 and what type of records are involved. 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 a USB key, CDs, and DVDs;
- to recall emails and/or requesting recipients to destroy the email containing personal information/personal health information;
- to immediately take down personal information/personal health information if it was posted online.

Investigating the Privacy Breach

Investigating the privacy breach to identify the root cause is key to understanding what happened. Identifying the root cause will help prevent similar breaches in the future.

1. What happened?
2. When did the privacy breach occur?
3. When and how did the public body/trustee learn of the breach (if different from above)?
4. What efforts have the public body/trustee made to contain the privacy breach?
5. Has the privacy breach been contained completely? Why or why not?
6. What personal information/personal health information was involved in the privacy breach?
7. Where did the privacy breach occur?
8. Who was involved?

9. Which employee(s) (if any) are involved or witnessed the privacy breach?

10. What type of personal information/personal health information is involved?

11. Who has been affected by this privacy breach?

Notice to Affected Individuals

Section 29.1 of FOIP and section 28.1 of LA FOIP requires that government institutions and local authorities take all reasonable steps to notify an individual of an unauthorized use or disclosure of that individual's personal information by the government institution or local authority if it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to the individual. For more information on what "real risk of significant harm" means, please refer to my office's blog entry entitled *Real Risk of Significant Harm*: https://oipc.sk.ca/real-risk-of-significant-harm/

For more information about how to notify affected individuals, please refer to pages 5 and 6 of *Privacy Guidelines for Government Institutions and Local Authorities* and pages 2 and 3 of *Privacy Guidelines for Trustees*.

1. Who are the affected individuals?

2. How many individuals are affected?

3. Has the public body identified the risks that the affected individuals will be exposed to because of the privacy breach?

4. Has the public body (or will the public body) notified the affected individuals? Why or why not?

Prevent Similar Privacy Breaches

Public bodies/trustee 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, and 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?
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.

Contact Information

If you have any questions or concerns about creating an internal privacy breach investigation report, please contact us:

306-787-8350 | toll free 1-877-748-2298

503 – 1801 Hamilton Street | Regina SK S4P 4B4

webmaster@oipc.sk.ca | www.oipc.sk.ca | @SaskIPC